UNIVERSIDADE DO EXTREMO SUL CATARINENSE

CURSO DE CIÊNCIA DA COMPUTAÇÃO

EDUARDO VIRTUOSO DOS SANTOS

IMPLEMENTAÇÃO DE CERTIFICAÇÃO DIGITAL EM UMA APLICAÇÃO CORPORATIVA: ESTUDO DE CASO NA UNESC

CRICIÚMA, NOVEMBRO DE 2006

EDUARDO VIRTUOSO DOS SANTOS

IMPLEMENTAÇÃO DE CERTIFICAÇÃO DIGITAL EM UMA APLICAÇÃO CORPORATIVA: ESTUDO DE CASO NA UNESC

Trabalho de Conclusão de Curso apresentado para obtenção do grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Profº. M.Sc. Rogério Antônio Casagrande

CRICIÚMA, NOVEMBRO DE 2006

Aos meus pais, pelo seu amor incondicional, apoio e incentivo em todos os momentos de minha vida.

AGRADECIMENTOS

A Deus, pela iluminação, proteção e inspiração concedida durante toda a minha trajetória.

Aos meus pais Adenor e Maria, pela grande dedicação e carinho dispensado.

Ao professor Rogério Antônio Casagrande, pela dedicação e paciência com a qual me orientou na realização deste trabalho, em especial pelos ensinamentos que me proporcionou.

A professora Merisandra Côrtes de Mattos, por suas importantes contribuições.

A minha namorada Leocádia, pelo carinho e compreensão em todos os momentos.

Ao colega Diego Paz Casagrande, pela amizade e companheirismo durante todo o curso.

Ao funcionário Diniz, pela sua ajuda na realização da pesquisa junto a Universidade.

Aos meus amigos que estiveram presente durante toda esta jornada.

A todos o meu muito obrigado!

RESUMO

Dado a quantidade cada vez maior de informações disponíveis em meio eletrônico, o conhecimento de técnicas para garantir a sua segurança deve ser explorada e difundida. Desse modo, esta pesquisa tem por finalidade o aprofundamento do conhecimento acerca da Certificação Digital, através das infra-estruturas de chaves públicas (ICP). São abordadas a ICP Brasil, que agrega validade jurídica aos certificados e a ICP EDU, voltada para utilização no meio acadêmico. Com a análise das arquiteturas disponíveis e dos formatos e padrões de certificados digitais existentes, este trabalho objetiva agregar uma maior segurança ao aplicativo Diário *On-Line* desenvolvido pela Universidade do Extremo Sul Catarinense (Unesc), através da implementação de certificação digital no servidor que abriga este sistema. Desta forma, conferem-se autenticidade, confidencialidade e sigilo na troca de informações.

Palavras-chave: Criptografia; Infra-estrutura de Chaves Públicas (ICP); Certificação Digital; Certificados Digitais.

ABSTRACT

Considering that the increasing quantity of available information in electronic field, the technician knowledge to assegure its security must be explored and spread out. Therefore, the main of this study is to deepen the Digital Certification knowledge, by the public key infrastructures (ICP). The study approaches the ICP Brazil, which associates legal validity to the certifyd and the ICP EDU, that is concerned about the academic utilization. With the available architectures analysis and existing digital certifyd forms and standards, this study has the objective of associating an increase in security to the On-Line Daily applicatiory desenvolved by Universidade do Extremo Sul Catarinense (UNESC), by the server digital certification implementation that supports this system. Then, confering autenced, confidential and private change information.

Key-words: Cryptography, Public Key Infrastructures (PKI); Digital Certification; Digital certifyd.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

AC	Autoridade Certificadora
AR	Autoridade Registradora
CEF	Caixa Econômica Federal
CSR	*Certificate Signing Request*
DES	*Data Encryption Standard*
DP	Diretório Público
DPC	Declaração de Práticas de Certificação
DSA	*Digital Signature Algorithm*
DSS	*Digital Signature Standard*
FGTS	Fundo de Garantia do Tempo de Serviço
HMAC	*Hashed Message Authentication Code*
HTTPS	*HyperText Transfer Protocol Secure*
ICP	Infra-Estrutura de Chave Pública
ITI	Instituto Nacional de Tecnologia da Informação
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
MD2	*Message Digest 2*
MD4	*Message Digest 4*
MD5	*Message Digest 5*
PC	Política de Certificados
PROUNI	Programa Universidade para Todos
SHA	*Secure Hash Algorithm*
SPB	Sistema de Pagamentos Brasileiro

SERPRO	Serviço Federal de Processamento de Dados
SRF	Secretaria da Receita Federal
UNESC	Universidade de Extremo Sul Catarinense

SUMÁRIO

1 INTRODUÇÃO

A certificação digital é considerada uma ferramenta de segurança extremamente eficaz na identificação de origem e destino das informações que trafegam na Internet.

A Universidade do Extremo Sul Catarinense (Unesc), atuando no ambiente virtual, percebe a necessidade de se utilizar da certificação digital. Necessita certificar seus servidores para fornecer informações e serviços com alto nível de segurança e oferecer maior confiabilidade no seu relacionamento com os funcionários e alunos, bem como realizar transações com entidades financeiras e governamentais que exijam certificação. Pode-se citar como exemplo o programa Universidade para Todos (ProUni), que exige assinatura digital em todos os documentos emitidos.

A fim de oferecer para a Universidade todas as funcionalidades da certificação digital, será estudada a arquitetura da Infra-estrutura de Chaves Públicas Brasileira (ICP Brasil), a Infra-estrutura de Chaves Públicas Educacional (ICP Edu) e os certificados digitais oferecidos no mercado.

Ao final será proposto e implementado certificação digital de um serviço na Unesc. Serão estudados os requisitos necessários para obtenção da certificação digital e as especificações dos certificados oferecidos pelas Autoridades Certificadoras.

1.1 OBJETIVO GERAL

Levantar as possibilidades de uso e aplicar certificação digital em um serviço da Unesc.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

a) compreender os fundamentos da criptografia;

b) conhecer a arquitetura da ICP Brasil e ICP Edu;

c) conhecer os tipos de certificados digitais oferecidos no mercado;

d) conhecer a legislação aplicada;

e) identificar os serviços nos quais é aplicável a certificação digital;

f) realizar um estudo de caso de certificação digital na Unesc;

g) certificar um serviço da Unesc.

1.3 JUSTIFICATIVA

A Internet tornou-se uma grande ferramenta para realização de comércio. Produtos e serviços podem ser adquiridos ou contratados rapidamente por qualquer usuário. Também se revelou uma grande rede de comunicação entre pessoas físicas, pessoas jurídicas e governo. Com esse crescimento do uso da Internet para todo tipo de transações e serviços eletrônicos, aumenta também a preocupação com a privacidade e a segurança. A assinatura digital, através da certificação digital agrega segurança e confiabilidade às transações eletrônicas.

O Certificado Digital é um documento criptografado que contém informações necessárias para identificação de uma pessoa física ou entidade jurídica. Como este certificado é fornecido por uma Autoridade Certificadora, qualquer conteúdo eletrônico que foi assinado digitalmente tem garantia de autenticidade de origem.

Motivado pelo interesse em ampliar os conhecimentos científicos na área de segurança e criptografia, foi realizado esta pesquisa e ao final proposto uma implementação de certificação digital para um serviço da Unesc.

Ao fazer uso dos certificados digitais na Universidade, uma variedade de aplicações possibilitará seu reconhecimento como uma organização de vanguarda e com uma política de segurança apropriada para seu objetivo maior de promover o desenvolvimento regional.

A pesquisa voltada à área da certificação digital tende a reforçar o quanto esta tecnologia está se tornando indispensável às organizações e a população em geral, pois pode proporcionar segurança e praticidade para qualquer tipo de transações feitas em meio eletrônico.

2 CRIPTOGRAFIA

A escrita cifrada é uma arte muito antiga. Logo que o homem aprendeu a escrever, sentiu a necessidade de escrever textos secretos ou em algumas ocasiões, esconder o que foi escrito. No início não havia muitas pessoas que sabiam ler, portanto pouca necessidade de esconder os textos. Lentamente foram surgindo várias técnicas e códigos usados para tornar os textos secretos (CARVALHO, 2001).

2.1 HISTÓRICO

Os sistemas antigos de criptografia eram baseados em técnicas de substituição e de transposição. A substituição consiste na troca de cada letra ou grupo de letras de uma mensagem de acordo com a tabela de substituição e pode ter as seguintes variações (CARVALHO, 2001):

a) **substituições simples ou monoalfabética:** é o tipo de cifra em que cada letra da mensagem é substituída por outra, baseada em um deslocamento da letra original dentro do alfabeto. Geralmente esta relação de substituição é fixa, por exemplo, substituía a letra “A” por “D”, “B” por “E” e assim por diante. Só aqueles que sabiam que a solução era deslocar três letras à frente poderiam decifrar a mensagem. A invenção deste sistema é atribuída ao imperador romano Júlio César;

b) **substituição monofônica:** funciona como a substituição monoalfabética, mas cada caractere da mensagem original pode ser mapeado para um ou vários caracteres na mensagem cifrada;

c) **substituição polialfabética:** consiste em utilizar várias cifras de substituição simples, em que as letras ou blocos da mensagem são substituídos por valores diferentes;

d) **substituição de poligramos ou blocos:** utiliza um grupo de caracteres ao invés de um único caractere individual para a substituição da mensagem;

e) **substituição por deslocamento:** ao contrário da cifra de César, não usa um valor fixo para a substituição de todas as letras. Cada letra tem um valor associado para a rotação através de um critério.

A transposição baseia-se na mistura dos caracteres da mensagem. Por exemplo, uma mensagem que é escrita normalmente em uma tabela (linha após linha) e ao ser enviada é lida coluna por coluna (CARVALHO, 2001).

No passado recente estas técnicas foram largamente utilizadas em guerras e conflitos para comunicação secreta entre exércitos e aliados. No início do século XX vários mecanismos eletromecânicos foram construídos em todo o mundo com a finalidade de codificar mensagens enviadas por telégrafo ou por rádio.

Train (2005) comenta que com a evolução dos meios de comunicação, a criptografia passou a ser sua ferramenta principal de segurança, sendo amplamente utilizada devido ao grande número de mensagens que circulam em diversos ambientes e sistemas.

Com relação a esta afirmação, Silva (2004) acrescenta que a criptografia possibilita a confidencialidade das informações, protegidas pela encriptação, e a integridade do conteúdo, assegurada pela autenticação.

2.2 O OBJETIVO DA CRIPTOGRAFIA

A palavra criptografia é composta dos termos gregos *kryptos* (secreto, oculto, ininteligível) e *grapho* (escrita, escrever). Consiste na ciência e na arte de se comunicar secretamente. Segundo Houaiss (2001), criptografia é o "conjunto de princípios e técnicas empregados para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas". Portanto, é uma forma de se tornar uma mensagem incompreensível, permitindo apenas ao destinatário desejado ler o texto original com clareza.

Train (2005) informa que para tornar uma mensagem legível em um texto cifrado utiliza-se um conjunto de operações que é chamado de algoritmo. Os sistemas modernos de criptografia consistem de dois processos complementares, o processo de encriptação que é utilizado para criar a mensagem cifrada e o processo inverso, chamado de desencriptação, que será realizado pelo destinatário para recuperar a mensagem original. Se o texto cifrado for interceptado por um terceiro, chamado de inimigo, deverá permanecer ininteligível. A informação que o remetente e o destinatário conhecem e que será utilizada para encriptar e desencriptar a mensagem é chamada de chave.

Com relação a esta definição Carvalho (2001) comenta que nem sempre a chave do remetente será igual a do destinatário, mas elas estarão sempre relacionadas.

O objetivo da criptografia é tornar impossível a recuperação da mensagem original a partir de um texto cifrado sem a chave correspondente e, além disso, dificultar ao máximo a chance de que se descubra sem autorização a chave que tornaria isso possível. A tendência atual é que sejam utilizados algoritmos conhecidos e largamente testados, de eficácia comprovada, sendo que a segurança reside totalmente

na chave secreta, que deve ter tamanho suficiente para evitar sua quebra por teste exaustivo, pois conhecendo o algoritmo, este pode ser usado para combinar todos os valores possíveis da chave secreta (SILVA, 2004).

Os algoritmos criptográficos são classificados em dois grupos que se diferenciam pela forma que utilizam as chaves criptográficas. São eles: algoritmos simétricos e algoritmos assimétricos.

2.3 ALGORITMOS SIMÉTRICOS

Estes algoritmos são caracterizados por utilizarem a mesma chave criptográfica para a encriptação e para a desencriptação. Esta chave deve ser secreta, de conhecimento exclusivo do remetente e do destinatário da informação, que deverão compartilhar a chave antecipadamente em um ambiente seguro. Este é o grande problema deste método, pois a chave tem que ser entregue aos participantes de um modo seguro, por exemplo, um encontro pessoal e as transações só poderão ser realizadas depois disso (SILVA, 2004).

A Figura 1 apresenta o fluxo da informação nos algoritmos de chave simétrica conforme mostra Stallings (1998).

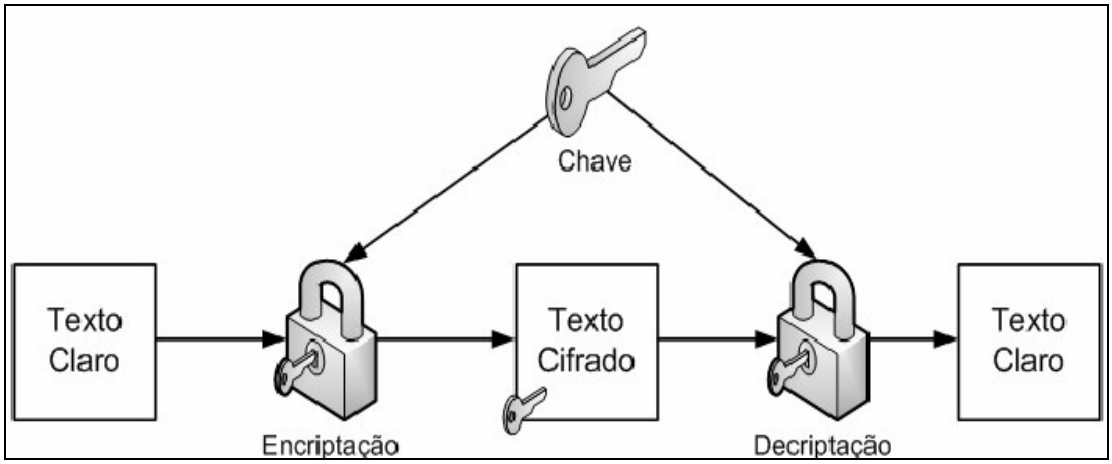

Figura 1. Criptografia Simétrica
Fonte: Adaptado de STALLINGS, W (1998, tradução nossa)

Silva (2004) lembra que pelo fato da chave criptográfica ser a mesma para os dois lados, este sistema possibilita o repúdio de uma transação, que acontece quando um lado acusa o outro de ter usado a chave para realizar uma transação em seu nome, indevidamente. E por necessitar de uma chave para cada par de participantes, a quantidade de chaves pode tornar algumas aplicações inviáveis neste sistema.

Contudo, estes algoritmos são projetados para serem bastante rápidos, possibilitando uma grande quantidade de chaves diferentes e seus melhores sistemas devem impossibilitar que se decifrem os dados sem ter conhecimento da chave secreta. Em outras palavras, não é necessário manter o algoritmo secreto, deve-se manter apenas a chave secreta. (STALLINGS, 1998, tradução nossa). Portanto, a segurança depende basicamente da chave escolhida e não do algoritmo.

Existem diversos algoritmos de chave simétrica em uso atualmente. Alguns destes algoritmos mais comuns no campo da segurança são (CARVALHO, 2001):

a) **DES:** o *Data Encryption Standard* foi adotado como padrão pelo governo dos Estados Unidos em 1977. É um algoritmo de bloco que usa uma chave de 56 bits e pode ser usado para várias finalidades. O DES é um algoritmo poderoso, mas pode ser quebrado por um ataque de força

bruta, ou seja, uma tentativa de se combinar e testar todas as chaves possíveis. Mesmo assim o DES resistiu por vários anos às tentativas de quebra. O que se pensa atualmente é que a vulnerabilidade não está no algoritmo em si, mas no tamanho da chave que ele usa;

b) ***Triple*-DES:** torna o DES pelo menos duas vezes mais seguro, usando o algoritmo de criptografia três vezes, com três chaves diferentes. Estima-se que usar o DES duas vezes com duas chaves diferentes não aumenta tanto a segurança, devido a um tipo teórico de ataque conhecido como *meet-in-the-midle* (encontro no meio), com o qual o inimigo tenta cifrar o texto limpo simultaneamente com uma operação do DES e decifrar o texto com outra operação, até que haja um encontro no meio;

c) ***Blowfish*:** é um algoritmo de criptografia em bloco, rápido, compacto e simples, citado por Bruce Schneier. Não é patenteado e foi colocado em domínio público;

d) **RC5:** é um algoritmo de bloco desenvolvido por Ronald Rivest em 1995. Este algoritmo pode ser parametrizado, ou seja, pode-se escolher os tamanhos dos blocos e das chaves e o número de iterações. Porém, apesar de esta condição permitir que se adapte o algoritmo as necessidades, deve-se escolher cuidadosamente os parâmetros para não resultar em um sistema criptográfico fraco.

2.4 ALGORITMOS ASSIMÉTRICOS

Com o desenvolvimento dos meios de comunicação à distância, tem-se a necessidade de um sistema criptográfico onde os lados não tenham a necessidade de se encontrar para combinar a chave secreta. Com o intuito de atender a esta necessidade, surgiu em 1976 o conceito dos algoritmos assimétricos, também conhecidos como algoritmos de chave pública ou criptografia de chave pública. Nestes sistemas, não é necessária a troca de chaves entre os usuários, pois elas são relacionadas em diretórios públicos (BUCHMANN, 2002).

Os algoritmos assimétricos necessitam de pares de chaves, ou seja, a mensagem codificada com a chave 1 de um par somente poderá ser codificada com a chave 2 deste mesmo par. As duas chaves utilizadas neste método são chamadas de chave pública e chave privada. A chave pública fica a disposição de qualquer um que a queira conhecer, já a chave privada é de conhecimento único de seu dono. Apenas com a chave pública é impossível descobrir qual seria a chave privada do destinatário (TRAIN, 2005).

Neste método o remetente codifica a mensagem com a chave pública da pessoa que a receberá e esta mensagem poderá ser decodificada apenas pelo destinatário, pois somente ele possui a chave privada relacionada à chave pública que originou o documento. Da forma inversa, o remetente pode também codificar a mensagem com sua chave privada e enviá-la ao destinatário que utilizará a chave pública do remetente para decodificar a mensagem. Neste caso o destinatário terá certeza da origem da mensagem (SILVA, 2004).

A Figura 2 mostra o fluxo da informação nos algoritmos de chave assimétrica de acordo com Stallings (1998).

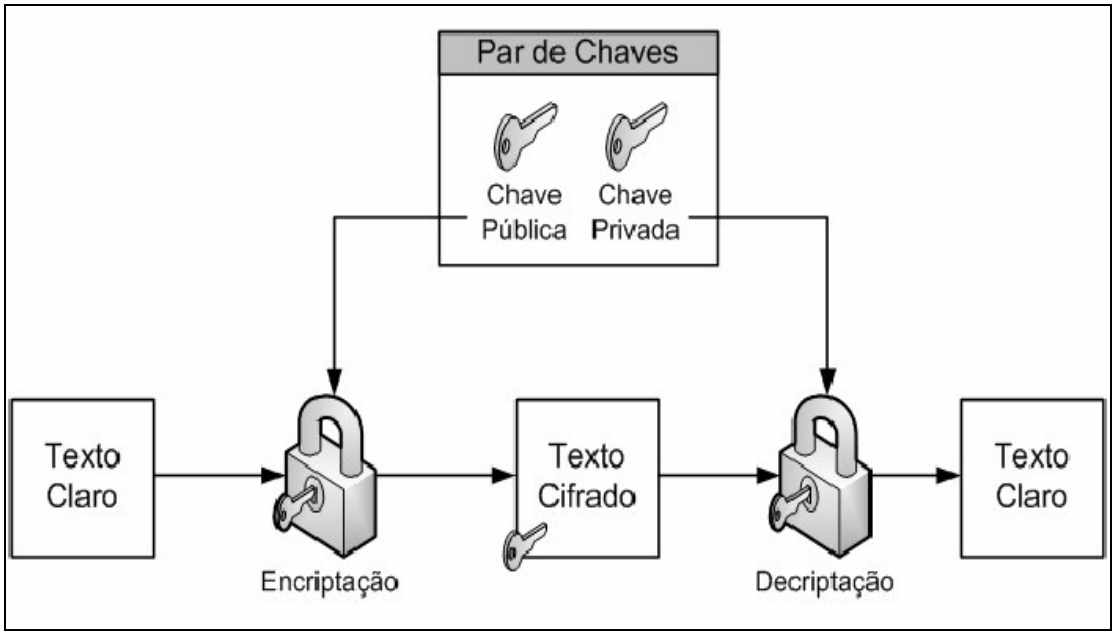

Figura 2. Criptografia Assimétrica
Fonte: Adaptado de STALLINGS, W (1998, tradução nossa)

Alguns dos principais sistemas de chaves pública em uso são os seguintes:

a) **RSA:** o sistema RSA tem este nome em referência aos sobrenomes de seus inventores Rivest, Shamir e Adleman. Segundo Buchmann (2002) este foi o primeiro sistema de chave pública e ainda é o mais importante. Com relação a este sistema, Carvalho (2001) acredita que é extremamente forte, quando usado adequadamente e informa que ele baseia-se no fato de que é extremamente difícil fatorar números muito grandes. A sua chave pode ser de qualquer tamanho, dependendo da implementação utilizada. O RSA pode ser usado para codificar informações como também para servir de base a um sistema de assinatura digital;

b) **Diffie-Hellman:** esse protocolo em si não é um criptossistema, é um método para troca de chaves secretas em canais inseguros e serve como base para o sistema ElGamal, que será descrito a seguir. As duas partes estabelecem certos valores numéricos comuns e cada uma delas cria

uma chave. As transformações matemáticas das chaves são intercambiadas. Cada parte calcula então uma terceira chave, chamada de chave de sessão que não pode ser descoberta facilmente por um inimigo que conheça os valores trocados. Todos podem ouvir a troca de chaves, mas a informação obtida não pode ser usada para construir a chave secreta (BUCHMANN, 2002);

c) **ElGamal:** está intimamente relacionado a troca de chave Diffie-Hellman. Segundo Carvalho (2001), este algoritmo foi criado inicialmente para implementar assinaturas digitais, mas pode ser usado também para codificar e decodificar mensagens. Seu algoritmo é baseado em exponenciação e aritmética modular. Envolve a manipulação matemática de grandes quantidades numéricas. O sistema é composto por um gerador de chaves, um algoritmo de encriptação e um algoritmo de desencriptação.

d) **DSS:** o *Digital Signature Standard* (Padrão de Assinatura Digital) foi publicado pelo governo dos Estados Unidos para ser usado como padrão federal em assinaturas digitais e é baseado no DSA - *Digital Signature Algorithm*, traduzido como Algoritmo de Assinatura Digital (CARVALHO, 2001). Difere do RSA na medida em que usa um algoritmo matemático diferente, que se baseia na dificuldade que existe em inverter uma operação exponencial matemática. Se comparado com o RSA, tem a desvantagem de exigir mais recursos por parte do computador sem ter uma maior força criptográfica (FORD; BAUM, 2000, tradução nossa);

2.5 ASSINATURAS DIGITAIS

Um obstáculo que se encontrou na utilização de documentos eletrônicos em negócios foi a impossibilidade de subscrevê-los. Silva (2004) lembra que quando se lança no papel o nome, firma ou sinal, de próprio punho, este documento tem um valor no sistema jurídico. O ato de assinar comprova o recebimento, a obrigação e a ciência dos termos contidos em um documento. Quem o assina se obriga e pode ser forçado a cumprir tais termos. A assinatura manual também atesta a identidade do signatário, pois é um sinal único e exclusivo de uma pessoa e graças a esta exclusividade comprova a autoria do documento. Mas no caso de documentos eletrônicos não bastaria simplesmente colocar uma marca para autenticá-lo, pois esta marca, ao contrário da assinatura manual poderia ser facilmente copiada ou fraudada. Conforme alerta Train (2005), é preciso garantir que a posse ou conhecimento desta assinatura seja exclusivamente do subscritor e da mesma forma garantir a proteção e a guarda do repositório de assinaturas.

Com base nestes princípios surgiram as assinaturas digitais, que são usadas para que uma entidade possa assinar digitalmente um documento. Da mesma forma que a assinatura manuscrita em um papel, a assinatura digital é utilizada para identificar de maneira irrecusável seu autor. A assinatura não é usada para proteger uma mensagem e sim para garantir a origem do documento (CARVALHO, 2001).

A geração de assinaturas digitais e sua validação dependem de algoritmos específicos que são baseados nos fundamentos da criptografia assimétrica. Neste pensamento Carvalho (2001) acrescenta que a chave privada, no caso, é algo que quem assina usa, e a chave pública é o que se deve usar para verificar a autenticidade da assinatura. Em outras palavras, para produzir uma assinatura digital sobre um

documento eletrônico, este é submetido ao algoritmo de geração de assinatura junto com a chave privada de quem está assinando. Na validação desta assinatura o algoritmo de verificação de assinatura utiliza a chave pública do suposto signatário para avaliar a autenticidade da assinatura, que somente é considerada autêntica caso tenha sido produzida utilizando a chave privada respectiva a esta chave pública.

2.5.1 Função *Hashing*

Train (2005) lembra que a assinatura digital obtida através do uso da criptografia assimétrica ou de chave pública não pode ser usada, na prática, de forma isolada, do modo como foi didaticamente descrito anteriormente. Depende de um mecanismo fundamental para seu emprego adequado. Este mecanismo é a função *Hashing*. Sua utilização é necessária devido à lentidão dos algoritmos assimétricos, em geral muito mais lentos que os simétricos.

Carvalho (2001) destaca que as funções *hash* são diferentes das funções normais de encriptação por não possuírem chave, e por serem irreversíveis. Por este motivo são consideradas ferramentas poderosas.

Como na prática é inviável utilizar puramente algoritmos de chave pública para assinaturas digitais, é empregada uma função *hashing*, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, que pode ter qualquer tamanho. Este valor é chamado de *digest*, valor *hash* ou ainda de resumo. No passo seguinte, o resumo é codificado com a chave privada do emissor da mensagem, gerando um arquivo eletrônico que representa a assinatura digital dessa pessoa. A partir daí esta assinatura digital gerada é anexada ao documento que será enviado

eletronicamente. Assim, a função *Hashing* oferece agilidade nas assinaturas digitais, além de integridade confiável (TRAIN, 2005).

Carvalho (2001) observa que qualquer pessoa pode verificar a autenticidade da mensagem, calculando a função *hashing* novamente e comparando com o resultado incluído na assinatura digital, porém não será capaz de falsificar a mensagem.

Uma boa função *hash* deve possuir como característica o chamado “efeito avalanche”. Isto significa que qualquer pequena mudança no arquivo de entrada produz uma grande e imprevisível mudança no resumo (CARVALHO, 2001).

Uma assinatura digital é dinâmica por natureza, única para cada mensagem assinada. A informação na mensagem enviada, mais a chave privada que o emissor necessita para codificar a mensagem, é parte integrante da assinatura digital e única devido aos complexos algoritmos matemáticos utilizados. Qualquer tentativa de intercepção e alteração da mensagem original irão levar invariavelmente a uma falha no momento da verificação da assinatura inicial. Esta característica significa que se deve ter cuidado para que a assinatura digital não seja reutilizada (STINSON, 1995, tradução nossa). Para tanto as assinaturas digitais podem ser aliadas também à datação eletrônica, que pode ser útil para comprovar que um documento foi assinado em um tempo específico. De outra forma, em um caso onde houver o comprometimento da chave privada de uma pessoa, torna-se impossível que elementos maliciosos que tenham tido acesso àquela chave privada assinem documentos em seu nome.

Ao ser projetada, uma função *hash* deve atender a determinadas propriedades, citadas por Stallings (1998, tradução nossa):

a) **compressão:** aplicando a função h sobre um bloco de dados x de qualquer tamanho, resultará em uma saída y de tamanho fixo;

b) **fácil computação:** tendo a função h e a entrada x, é relativamente fácil computar h(x);

c) **caminho único:** é impraticável computacionalmente deduzir o valor de entrada x a partir do valor de saída y;

d) **fraca resistência à colisão:** dado x, é impraticável encontrar um valor x´ tal que h(x) = h(x´);

e) **forte resistência à colisão:** é impraticável computacionalmente encontrar duas entradas distintas, x e x´, que produzam o mesmo resumo.

As principais funções de codificação de mensagem que foram propostas e estão em uso, são citadas por Garfinkel e Spafford (1999):

a) **HMAC:** o *Hashed Message Authentication Code* (Código de Autenticação de Mensagens por Confusão), é uma técnica que usa uma chave secreta e uma função de codificação para criar um código secreto de autenticação de mensagem. O método HMAC reforça uma função de codificação existente de forma a torná-la resistente a ataques externos, mesmo que a própria função de codificação esteja de certa forma comprometida;

b) **MD2:** *Message Digest* 2 (Codificação de Mensagem 2), proposto por R. Rivest. Esta é a mais segura das funções de codificação de mensagem de Rivest, porém demora mais para calcular. Produz uma codificação de 128 *bits*;

c) **MD4:** *Message Digest* 4 (Codificação de Mensagem 4), também proposto por R. Rivest. Este algoritmo de codificação de mensagem foi desenvolvido como uma alternativa rápida para o MD2, mas para tanto

enfraqueceu a segurança em alguns pontos. Ou seja, é possível encontrar dois arquivos que produzem o mesmo código MD4 sem uma pesquisa de força bruta. O MD4 produz uma codificação de 128 *bits*;

d) **MD5:** *Message Digest* 5 (Codificação de Mensagem 5). O MD5 é uma modificação do MD4 que inclui técnicas para torná-lo mais seguro. Embora largamente usado, foram descobertas algumas falhas nele que permitiam calcular alguns tipos de colisão;

e) **SHA:** o *Secure Hash Algorithm* (Algoritmo de Confusão Seguro), desenvolvido pelo governo dos Estados Unidos para ser utilizado como padrão de assinatura digital do seu instituto nacional. Logo após sua publicação, anunciou-se que não era próprio para uso sem que fosse incluída uma pequena modificação;

f) **SHA1:** o SHA1 incorpora pequenas mudanças com relação ao SHA e produz uma codificação para 160 *bits.*

Por fim, Carvalho (2001), informa que o algoritmo padrão americano para geração e verificação de assinaturas digitais definido pelo Instituto Nacional de Padrões e Tecnologia Americano (NIST) é o *Digital Signature Algorithm* (DSA) que utiliza o algoritmo SHA-1 para geração de resumos.

Contudo, além do DSA o algoritmo RSA em conjunto com o algoritmo SHA-1 é também muito utilizado na geração de assinaturas digitais (STALLINGS, 1998, tradução nossa).

Buchmann (2002) cita que a assinatura digital também pode ser usada para identificar os participantes numa transação, através da utilização do método de “desafio resposta”. Neste método, um dos participantes sorteia e envia para o outro uma mensagem aleatória, que é o desafio. O outro tem de assinar digitalmente o mesmo e

devolver como resposta, que por sua vez é verificada pelo primeiro com a chave pública do segundo, e o resultado comparado com o desafio original. Havendo a coincidência, o segundo participante tem sua identidade garantida. O processo pode ser também realizado do segundo para o primeiro, completando a autenticação de ambos os participantes. Esse método de autenticação é denominado autenticação forte em comparação ao método de senhas, utilizado para identificação dos participantes de uma interação em sistemas convencionais.

2.6 CONFIDENCIALIDADE, AUTENTICIDADE E NÃO REPÚDIO

No tocante à segurança da informação, Stallings (1998, tradução nossa) acredita que os principais serviços providos pela criptografia são:

a) **confidencialidade:** esta característica garante que as informações protegidas serão acessíveis exclusivamente pelas entidades autorizadas. Este acesso inclui além da leitura da informação, qualquer outro tipo de revelação ou publicação. Portanto esta informação não poderá ser interceptada por uma terceira parte não autorizada no processo de comunicação;

b) **autenticidade:** identifica de maneira segura uma entidade, assegurando a origem da comunicação. Não permite que seja fabricada uma mensagem onde o emissor tenta se passar por um usuário autêntico;

c) **não repúdio:** garante que uma entidade não possa negar uma ação praticada por ela. Como somente o assinante tem acesso a sua chave privada, não poderá contestar uma ação efetuada com a posse da mesma.

Com a impostação da assinatura digital, em um ambiente de chaves públicas, também se pode citar a segurança com a integridade das informações. Com relação a esta característica, Silva (2004) comenta que se a mensagem original sofrer alguma alteração enquanto transita em um meio não seguro, esta alteração será percebida ao se conferir a autenticidade da assinatura.

Finalmente, Train (2005) alerta que para trocar informações entre duas partes, autenticando o emissor e o receptor, torna-se necessário que os participantes conheçam e confiem na chave pública do respectivo interlocutor. É preciso que o repositório destas chaves seja confiável. Neste contexto, foi desenvolvida a infra-estrutura de chave pública.

3 INFRA-ESTRUTURA DE CHAVE PÚBLICA – ICP

Sendo que nos sistemas de criptografia assimétrica as chaves públicas não precisam ser mantidas em segredo, o gerenciamento destas chaves torna-se mais simples do que nos sistemas simétricos (BUCHMANN, 2002). De fato, estas chaves, como o próprio nome sugere, devem ser de acesso público. Porém, deve-se protegê-las contra falsificação e abuso por entidades mal intencionadas. Quando se trabalha com um grupo pequeno e confiável, em uma rede fechada, pode ser viável manter um banco de dados com as chaves públicas individuais, onde cada membro pode verificar sua autenticidade. Porém em uma rede aberta, a idéia que se tem quanto ao meio e ao repositório de chaves públicas é de que são inseguros e não confiáveis. Isto porque se desconhece os seus mantenedores e qualquer um pode alegar ser o que desejar, sendo impossível verificar a autenticidade dessa informação no meio virtual.

Para impedir que isto aconteça, faz-se necessária uma entidade confiável para abrigar este banco de dados. Com este fim são configuradas as infra-estruturas de chaves públicas. Esta é uma solução que permite que haja um interlocutor comum em que os participantes possam confiar e que seja reconhecido como idôneo e seguro (SILVA, 2004).

A Infra-estrutura de Chave Pública ou ICP é o correspondente no Brasil à *Public Key Infrastructure* (PKI), um conjunto de técnicas, práticas e procedimentos elaborados para suportar um sistema criptográfico com base em certificados digitais. Estes procedimentos são responsáveis por criar, gerenciar, armazenar e distribuir certificados digitais de chave pública. Tais certificados são documentos eletrônicos que associam de forma segura o valor de uma chave pública a uma pessoa ou entidade e

serão abordados adiante. Sua emissão é feita por uma Autoridade Certificadora, a qual assina o certificado a fim de conferir veracidade aos seus dados (ITI, 2006).

3.1 AUTORIDADE CERTIFICADORA

A Autoridade Certificadora (AC) é a entidade responsável pela emissão de certificados digitais e pelo controle dos certificados revogados e expirados. Esses certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, empresa, organização, computador, entre outros. A emissão de um certificado digital se inicia quando a AC recebe uma solicitação contendo os dados identificadores da entidade solicitante e sua chave pública. Após comprovar a veracidade dos dados, de acordo com as políticas estabelecidas, o certificado digital é assinado pela autoridade. Então uma cópia do certificado é enviada ao solicitante e outra ao diretório público (SILVA, 2004).

De acordo com Buchmann (2002) recomenda-se que o solicitante não conheça sua chave secreta, desta forma não poderá informar a outras pessoas sobre esta chave. Sendo assim a chave privada geralmente é armazenada em um dispositivo seguro, conforme será descrito posteriormente. Após a emissão e o recebimento do certificado, o solicitante passa a ser denominado assinante dos serviços disponibilizados pela infra-estrutura de chaves públicas.

Silva (2004) informa que a revogação de um certificado digital é de responsabilidade exclusiva da AC, podendo ser solicitada pelo assinante ou motivada por uma situação específica, como por exemplo, o comprometimento da chave privada. Os certificados revogados por uma autoridade certificadora são inseridos em uma Lista de Certificados Revogados (LCR) emitida e assinada pela própria autoridade. Estas

listas são disponibilizadas publicamente, possibilitando que usuários de certificados digitais verifiquem se um certificado digital está ou não revogado, tanto para gerar a assinatura como para conferir. As atualizações desta lista devem ser efetuadas em um período de tempo adequado a fim de evitar que certificados revogados sejam considerados válidos inadequadamente.

A segurança necessária a uma AC, tanto física quanto lógica, também é de extrema importância. Qualquer falha neste processo pode comprometer toda a estrutura de chaves públicas em que esta AC esteja envolvida. Ou seja, se alguma entidade conseguir invadir a base de dados de uma AC roubando a chave privada da mesma, poderá gerar certificados digitais e assiná-los com a chave privada que roubou. Contudo, uma infra-estrutura de chaves públicas tem sua proteção em caso de exposição da chave privada. Essa segurança exigida pela ICP é muito ampla e cara, mas necessária. Abrange tópicos que poucas empresas estão preparadas para implantar (SILVA, 2004).

3.2 AUTORIDADE REGISTRADORA

A Autoridade Registradora ou Autoridade de Registro (AR) é a entidade vinculada operacionalmente a uma determinada Autoridade Certificadora. Referindo-se a esta entidade Train (2005, p 23) cita que “Sua função é identificar e cadastrar usuários, em postos de atendimento que os mesmos possam comparecer e, a partir daí, encaminhar as solicitações de certificados para uma AC.” A averiguação e comprovação dos dados obedecem a políticas e padrões pré-definidos.

Algumas das maneiras utilizadas para a validação dos dados fornecidos pelo solicitante são as verificações de documentos e a solicitação da presença física do

mesmo. As solicitações de certificados para equipamentos ou organizações deverão ser solicitadas pela pessoa física legalmente constituída como responsável pela sua administração (SILVA, 2004).

Silva (2004) acrescenta ainda que em determinadas situações, uma AC pode delegar a função de AR a mais de uma entidade. Esta condição é útil para situações onde é necessário identificar usuários em regiões geograficamente distantes. A estas entidades dá-se o nome de Autoridade de Registro Local.

Com relação a responsabilidade das autoridades de registro, Train (2005) ressalta que é extremamente importante a correta identificação do usuário, pois após esta etapa, àquela entidade será reconhecida como legítima até o fim da vigência do certificado.

3.3 DIRETÓRIO PÚBLICO

O Diretório Público (DP) é a entidade que fica responsável pela publicação dos certificados digitais e das Listas de Certificados Revogados (LCR). É por meio destes diretórios que os usuários podem obter os certificados digitais que eles pretendem utilizar. O DP não contém mecanismos que garantam a autenticidade e integridade dos dados que ele armazena. Estes requisitos são obtidos pela verificação da validade da assinatura digital da Autoridade Certificadora em determinado certificado e pela consulta a LCR (SILVA, 2004).

3.4 ARQUITETURA DA ICP

A infra-estrutura de chaves públicas pode usar de várias formas para interligar suas Autoridades Certificadoras, sendo que a mais conhecida é o modelo hierárquico de relacionamento. Neste tipo de arquitetura, as AC são dispostas hierarquicamente, abaixo da AC Raiz que emite certificados para elas. Essas AC podem ainda, emitir certificados para as AC abaixo delas e assim por diante até chegar aos usuários finais (SILVA, 2004).

A respeito deste modelo, Silva (2004) afirma que nessa arquitetura, todas as AC confiam em uma AC central chamada de AC Raiz. Com exceção da AC Raiz, todas as outras possuem uma única AC superior. A Figura 3 representa este tipo de arquitetura.

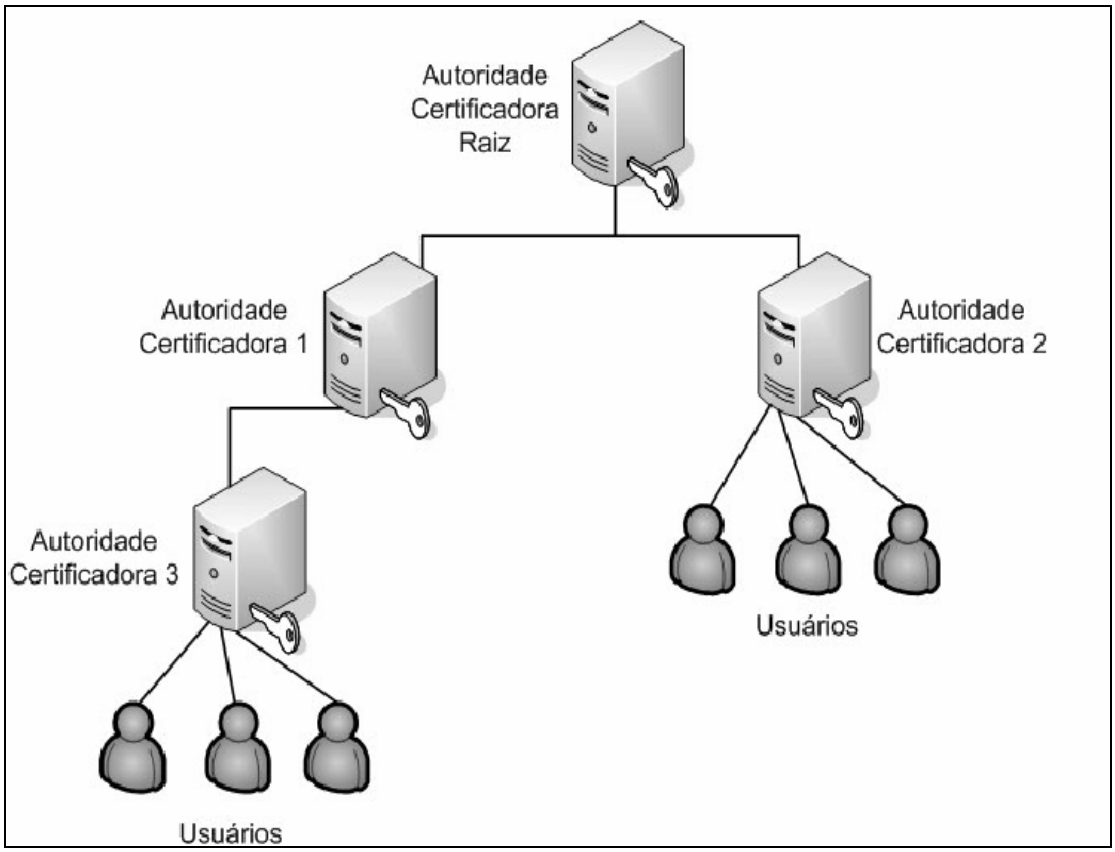

Figura 3. Arquitetura Hierárquica
Fonte: Adaptado de SILVA, L (2004)

A AC Raiz é o topo da hierarquia, portanto seu certificado é um certificado auto-assinado. Ela não é dependente de nenhuma outra AC, isso é necessário para garantir a validação da hierarquia das outras AC. A partir daí, todas as AC que forem criadas nessa estrutura terão seus certificados assinados pela AC Raiz (SILVA, 2004).

Outro modelo de relacionamento é a arquitetura mista, também conhecida como certificação cruzada ou distribuída, em que as AC idenpedentes autenticam-se mutuamente, emitindo certificados umas para as outras, resultando em uma mistura de relações de confiança (SILVA, 2004). A Figura 4 mostra esta arquitetura.

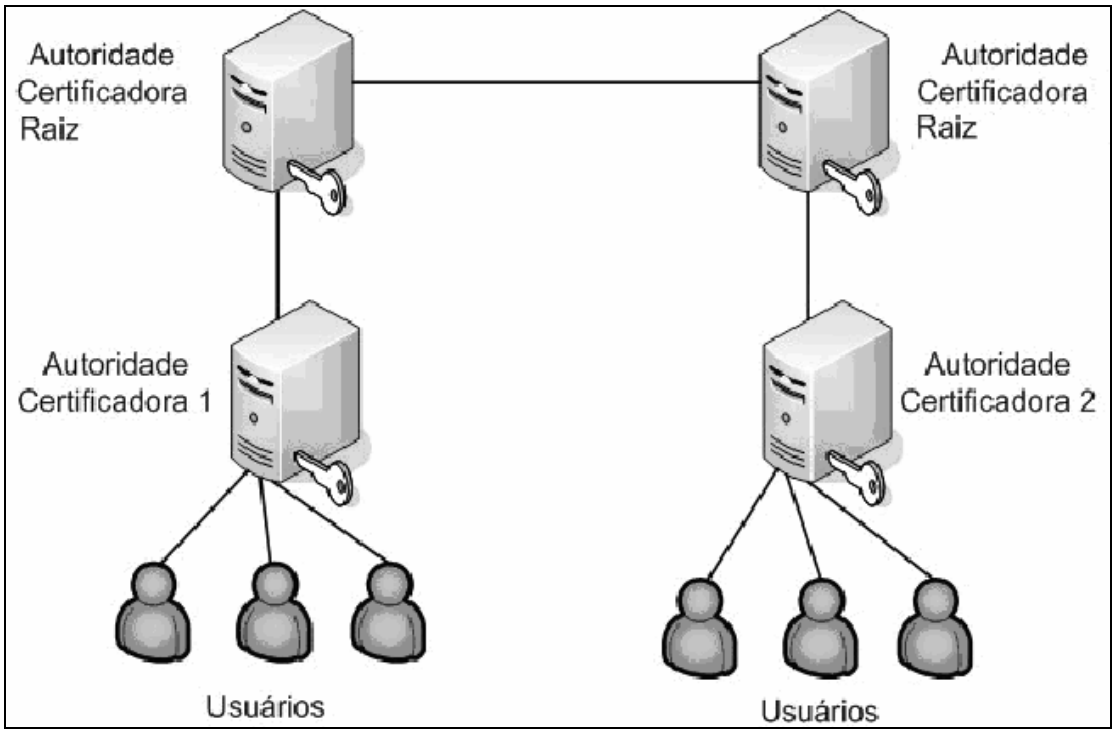

Figura 4. Arquitetura Mista
Fonte: Adaptado de SILVA, L (2004)

Silva (2004) ressalta que apesar de cada usuário confiar em uma única AC, as AC não se reportam unicamente a uma AC superior a ela, como acontece na arquitetura hierárquica. Na visão do usuário isso é transparente, mas para as AC isso muda, pois ela pode alcançar um usuário através mais de um caminho.

Existe também a arquitetura ponte, que serve para conectar as ICP de organizações independentemente de sua arquitetura. Isso acontece por meio da introdução de uma nova AC, chamada de AC Ponte, que tem como única finalidade, estabelecer relacionamentos entre ICP. A AC Ponte não pode emitir certificados, serve apenas para interconectar os usuários de cada ponta (SILVA, 2004).

3.5 ICP BRASIL

Para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, bem como aplicações de suporte, aplicações habilitadas que utilizem certificados digitais e a realização de transações eletrônicas seguras foi implementada a ICP Brasil. Ao definir sua estrutura foi adotada a arquitetura hierárquica, centralizada e vinculada ao Governo Federal, a ICP Brasil. Esta estrutura foi definida pela Medida Provisória 2.200-2, datada de 24 de agosto de 2001. Sua autoridade gestora de políticas é o Comitê Gestor (CG) da ICP Brasil, vinculado a Casa Civil da Presidência da República e composto por representantes da sociedade civil indicados pelo Presidente da República (BRASIL, 2001).

Segundo Silva (2004) é função do CG:

a) estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP Brasil em todos os níveis da cadeia;
b) aprovar políticas de certificados, práticas de certificação e regras operacionais;
c) credenciar e autorizar o funcionamento das AC e AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

d) identificar e avaliar as políticas de ICP Externas;

e) negociar, aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional;

f) certificar, quando for o caso, sua compatibilidade com a ICP Brasil, observando o disposto em tratados, acordos ou atos internacionais;

g) atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP Brasil;

h) garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Complementando, Silva (2004) informa que o objetivo da medida provisória foi de criar os primeiros níveis da estrutura ICP, o comitê gestor e a autoridade certificadora raiz. Os demais membros, como AC, AR e usuários foram incorporados com o tempo, de acordo com a necessidade e com o cadastramento de novas empresas a esta estrutura. O sistema da AC Raiz, valoriza o aspecto da interoperabilidade tecnológica que é obtida com a ampla distribuição de uma chave única pública, com a qual AC Raiz assinará os certificados das demais entidades credenciadas, criando assim uma cadeia de reconhecimento até o usuário final, titular do certificado.

À AC Raiz, primeira autoridade da cadeia de certificação, atribuiu-se os poderes para emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, executar atividades de fiscalização e auditoria das AC, AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo CG da ICP Brasil (BRASIL, 2001).

A AC Raiz da ICP Brasil é o Instituto Nacional de Tecnologia da Informação (ITI), autarquia pertencente à administração pública federal, ligado à Casa Civil da Presidência da República. A AC Raiz não tem poder para emitir certificados para o usuário final. Para este propósito existem as AC vinculadas a ela (ITI, 2006).

A Figura 5 mostra a estrutura atual da ICP Brasil de acordo com o ITI (2006).

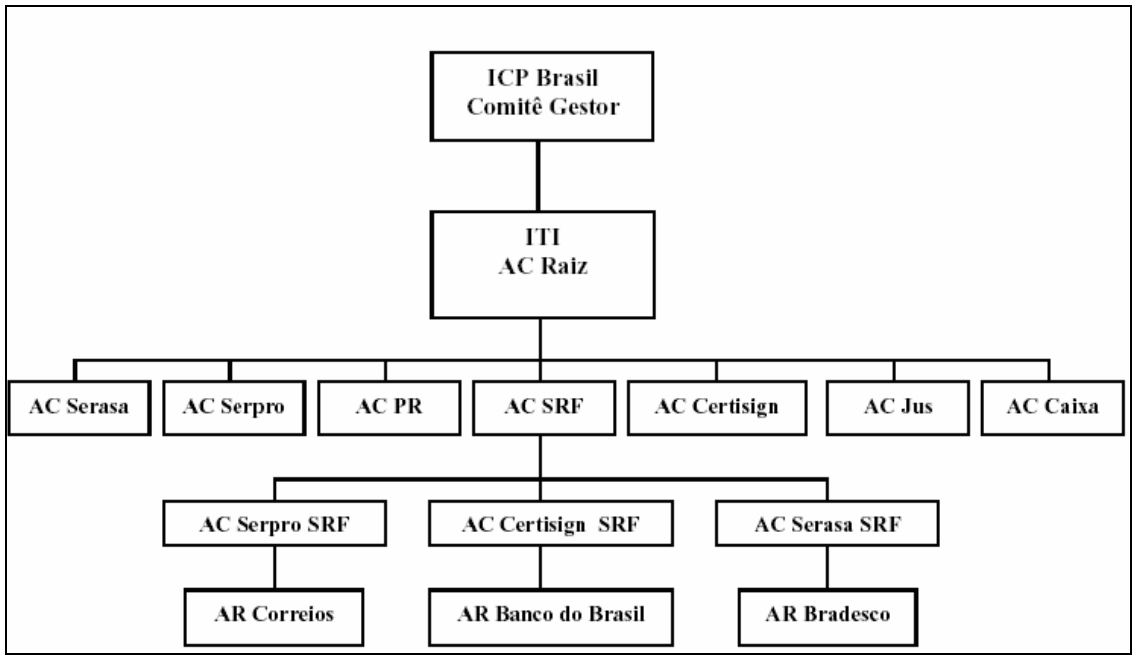

Figura 5. Estrutura da ICP Brasil
Fonte: ITI (2006)

Referindo-se a esta estrutura, o ITI (2006) informa sobre as AC que a compõe:

a) **Serasa:** a Serasa fornece a segurança dos certificados digitais para quase todos os grupos financeiros participantes do Sistema de Pagamentos Brasileiro (SPB);

b) **Serviço Federal de Processamento de Dados (SERPRO):** é a maior empresa pública de prestação de serviços em tecnologia da informação

do Brasil. Foi a primeira autoridade certificadora credenciada pela ICP Brasil;

c) **Presidência da República (AC PR):** foi criada em abril de 2002, por uma iniciativa da Casa Civil e tem como objetivo emitir e gerir certificados digitais das autoridades da Presidência da República, ministros de estado, secretários-executivos e assessores jurídicos que se relacionem com a Presidência;

d) **Secretaria da Receita Federal (SRF):** disponibiliza uma grande quantidade de serviços na internet, com o objetivo de simplificar as informações para os contribuintes e facilitar o cumprimento espontâneo das obrigações tributárias;

e) **Certsign:** empresa fundada em 1996 com foco exclusivamente no desenvolvimento de soluções de certificação digital para o mercado brasileiro. Através dela, importantes instituições vêm adotando a certificação digital nas mais diversas formas;

f) **Justiça (JUS):** reúne o Conselho da Justiça Federal (CJF), o Superior Tribunal de Justiça (STJ) e os cinco Tribunais Regionais Federais. Trata-se da primeira autoridade certificadora do Poder Judiciário;

g) **Caixa Econômica Federal (CEF):** atualmente única instituição financeira credenciada como AC na ICP-Brasil. Utiliza a tecnologia de certificação digital para prover a comunicação segura na transferência de informações referentes ao Fundo de Garantia do Tempo de Serviço (FGTS) e à Previdência Social, dentro do projeto Conectividade Social.

A ICP Brasil é formada por um sistema de credenciamento voluntário das entidades prestadoras de serviços, porém possui uma legislação em que a fiscalização e

supervisão da conformidade aos requisitos técnicos significam o controle detalhado e estrito da operação das AC credenciadas pela AC Raiz, incluindo autorização prévia para funcionamento. As AC credenciadas são auditadas pela AC Raiz antes de iniciarem seus serviços e durante sua atuação. Esta auditoria verifica se as exigências das normas da ICP Brasil são integralmente cumpridas. Após o credenciamento, persiste o dever das AC cumprirem todas as obrigações assumidas (ITI, 2006).

Com a instituição da ICP Brasil, criou-se a eficácia jurídica do documento eletrônico assinado com a utilização de certificado emitido no âmbito da ICP Brasil. Conforme dita a MP 2.200-2, os documentos eletrônicos assinados digitalmente com o uso de certificados digitais emitidos no âmbito da ICP Brasil têm a mesma validade jurídica dos documentos escritos com assinaturas manuais (SILVA, 2004).

Para os documentos assinados digitalmente com certificados emitidos fora do âmbito da ICP Brasil, a validade jurídica dependerá da aceitação das partes envolvidas, conforme determina a Medida Provisória (BRASIL, 2001).

Por fim, ressalta-se a facilidade de verificação do caminho de certificação. A parte destinatária do documento eletrônico poderá verificar o certificado do emitente, da AC que emitiu este certificado, da AC de nível superior e, assim sucessivamente até a verificação do certificado da AC Raiz, que é auto-assinado, tendo a segurança e a confiabilidade de toda a cadeia de certificados (ITI, 2006).

Silva (2004) discorre ainda sobre os documentos oficiais publicados para a ICP Brasil:

a) **política de segurança da ICP Brasil:** este documento foi publicado na segunda resolução do Comitê Gestor e define a política de segurança que deve ser adotada por qualquer entidade que participe da estrutura da ICP Brasil;

b) **Declaração de Práticas de Certificação (DPC):** expõe as regras operacionais das atividades de determinada autoridade certificadora. Entre outras informações, contêm os procedimentos gerais para a identificação dos usuários de certificados digitais, obrigações das partes envolvidas e padrões técnicos;

c) **requisitos mínimos para as DPCs:** este documento estabelece os requisitos mínimos que devem obrigatoriamente estar contidos nas DPCs de todas as Autoridades Certificadoras integrantes da ICP Brasil;

d) **Políticas de Certificados (PC):** contêm detalhes específicos sobre cada tipo de certificado emitido por uma Autoridade Certificadora, como formato padrão e tamanho das chaves criptográficas associadas a ele.

3.6 ICP EDU

A Rede Nacional de Ensino e Pesquisa (RNP), ligada ao Ministério da Ciência e Tecnologia e que conecta computadores em mais de 800 instituições em todo o país, lançou no ano de 2003 uma chamada pública para financiamento de projetos, que apresentassem soluções viáveis para a implantação de uma infra-estrutura capaz de dar suporte ao uso de assinaturas digitais no cotidiano das universidades.

O projeto vencedor foi o Grupo de Trabalho ICP Educacional (GT ICP EDU) um Grupo de Trabalho resultante da união de pesquisadores da Universidade Federal de Santa Catarina (UFSC), Universidade Estadual de Campinas (Unicamp) e Universidade Federal de Minas Gerais (UFMG). Segundo Custódio, Graaf e Dahab (2003) a Infra-Estrutura de Chaves Públicas Educacional é um projeto para unificar as ICP no âmbito acadêmico brasileiro. O objetivo é facilitar o reconhecimento mútuo de

certificados emitidos por universidades ou outras organizações acadêmicas, assim facilitando a autenticação, autenticidade, integridade e não-repúdio nas comunicações. Esses certificados não precisam possuir validade jurídica, pois serão usadas apenas no meio acadêmico.

O projeto foi dividido em etapas, sendo que duas delas já foram concluídas. A primeira etapa realizada entre setembro de 2003 e dezembro de 2004 centrou-se no desenvolvimento de um conjunto de programas para emitir e gerenciar certificados. A segunda etapa concluída entre janeiro de 2005 e fevereiro de 2006, objetivou o desenvolvimento de um hardware para armazenar as chaves privadas de um servidor. A ultima etapa está trabalhando no desenvolvimento de software para armazenar a chave privada de um titular (CUSTÓDIO; GRAAF; DAHAB, 2003).

Com este GT, a RNP poderá estimular a aplicação da tecnologia de ICP no mundo acadêmico em âmbito nacional. Várias iniciativas isoladas têm surgido e a sua unificação será inevitável para que a utilização da tecnologia seja efetiva.

A exemplo da RNP, o ITI também procura estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital. Neste vetor, esta autarquia federal tem como sua principal linha de ação a popularização da certificação digital. A “carteira de identidade virtual”, que permite a identificação segura de uma mensagem ou transação em rede de computadores. Desta forma, poderá ajudar no atual processo de disseminação do uso de certificados digitais no país (ITI, 2006).

3.7 CERTIFICADOS DIGITAIS

As AC têm várias obrigações importantes, entre elas está o poder de emitir certificados digitais para pessoas físicas ou jurídicas, equipamentos e aplicações. A certificação amarra uma entidade com suas informações relevantes e para garantir sua autenticidade a AC assina o documento com sua chave privada. O passo seguinte a esta assinatura é a geração do par de chaves para a entidade. A chave pública é incluída no certificado e repassada para a AC. A chave privada ficará em poder da entidade. O certificado digital significa que alguém ou algo se apresentou à AC e provou sua autenticidade no momento de sua geração. Portanto, o certificado digital é um documento eletrônico assinado digitalmente que cumpre a função de associar uma pessoa ou entidade a uma chave pública. As informações públicas contidas num certificado digital são o que possibilita colocá-lo em repositórios públicos (SILVA, 2004).

Em outras palavras, o certificado digital é um documento eletrônico que pode ser utilizado para identificar uma entidade em transações virtuais. Como qualquer documento, ele contém informações sobre seu titular, por exemplo, nome, data de nascimento e endereço.

O certificado digital torna uma transação eletrônica realizada via internet mais segura, pois permite que as partes envolvidas se apresentem e possam comprovar a sua real identidade. Desta forma estão assegurados os princípios da autenticidade e o de não repúdio (ITI, 2006).

3.8 TIPOS DE CERTIFICADOS

Pelo fato do conceito da criptografia de chave pública estar disponível à comunidade há muitos anos, existem vários tipos de certificados no mercado. No decorrer dos anos muitas soluções foram desenvolvidas e apresentadas para atender diversas necessidades. À medida que o mercado de certificação digital foi se popularizando, as organizações que definem os padrões foram se mobilizando para propor especificações, com o objetivo de reunir o melhor de cada proposta. Apesar da variedade, o padrão que está se sobressaindo e está sendo usado pela ICP Brasil é o X.509, mais especificamente a versão 3, da *International Telecommunications Union* (ITU), que foi publicada em 2002 (SILVA, 2004).

A respeito deste padrão, Silva (2004) informa que sua primeira versão foi publicada em 1988, definindo um formato para os certificados digitais. Em 1993 este padrão foi revisado acrescentando-se dois campos e passou a sua versão 2. Porém, algumas deficiências ainda existiam, levando-se a criação da versão 3 que adiciona aos certificados os campos de extensão, sendo completada em 1996.

Os campos que compõe o padrão X.509 estão descritos a seguir (SILVA, 2004):

a) ***version*:** indica a versão do formato, podendo ser 1,2 ou 3;

b) ***serial number*:** número inteiro que é único desse certificado relativo à entidade que o emitiu;

c) ***signature*:** identifica o algoritmo utilizado para assinar o certificado;

d) ***issuer*:** identifica o nome distinto (*Distinguished Name*) com o qual a AC cria e assina esse certificado;

e) ***validity*****:** identifica o intervalo de tempo em que o certificado deve ser considerado válido, a menos que ele seja revogado por outra circunstância diferente do tempo;

f) ***subject*****:** indica o nome distinto do dono do certificado;

g) ***subject public key info*****:** informa o valor da chave pública do proprietário do certificado, bem como o identificador de algoritmo e qualquer outro parâmetro associado ao algoritmo pelo qual a chave deve ser utilizada;

h) ***issuer unique ID*****:** Campo opcional que contém um identificador único que é utilizado para exibir de maneira não-ambígua o nome da AC, em casos onde um mesmo nome foi reutilizado por diferentes entidades ao longo do tempo;

i) ***subject unique ID*****:** Campo opcional que contém um identificador único que é utilizado para exibir de maneira não-ambígua o nome do proprietário do certificado, em casos onde um mesmo nome foi reutilizado por diferentes entidades ao longo do tempo;

j) ***extensões*****:** as extensões possibilitam que uma AC inclua informação que normalmente não seria fornecida pelo conteúdo básico do certificado;

k) ***digital signature*****:** Identificador do algoritmo utilizado e a assinatura digital da AC que emitiu o certificado.

Silva (2004) acrescenta que as extensões possuem três componentes, um identificador, um sinalizador de criticidade e um valor. O identificador contém o formato e a semântica do campo valor. O sinalizador de criticidade indica a importância de extensão, quando este sinalizador estiver ligado, significa que a

informação é essencial para o uso do certificado. Portanto, se for encontrado um sinalizador de criticidade desconhecido, o certificado não deverá ser aceito.

3.9 MÍDIA ARMAZENADORA

Segundo Train (2005), existem dois tipos principais de mídias para o armazenamento das chaves privadas. São os cartões inteligentes ou *smart cards* e os *tokens*. Ambos são hardwares portáteis que funcionam como mídias armazenadoras. Em seus chips são armazenadas as chaves privadas dos usuários. O *smart card* assemelha-se a um cartão magnético, sendo necessário um aparelho leitor para seu funcionamento. Já o *token* assemelha-se a uma pequena chave e requer a utilização de uma porta USB. O acesso às informações neles contidas é feito por meio de uma senha pessoal, determinada pelo titular.

Para o seu correto funcionamento, as leitoras de *smart card* e os *tokens* necessitam da instalação de um software para permitir o reconhecimento destes dispositivos pela máquina em que serão utilizados (SILVA, 2005).

A Figura 6 mostra a estrutura de um *smart card* e a Figura 7 um exemplo de *token* USB.

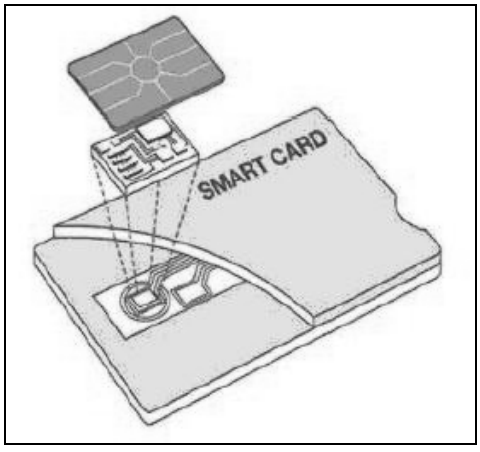

Figura 6. Estrutura do *smart card*
Fonte: TRAIN, S (2005)

Figura 7. Exemplo de *Token* USB
Fonte: CERTISIGN (2006)

3.10 NOMENCLATURA

As políticas de certificados definidas pela ICP Brasil são formas de se qualificar o certificado de acordo com a forma de geração ou armazenamento do mesmo. Além disso, a nomenclatura sugere o uso do certificado, Assinatura (A) ou Sigilo (S). Certificados de tipos A1, A2, A3 e A4 são utilizados em aplicações como confirmação de identidade na internet, correio eletrônico, transações *on-line*, redes privadas virtuais e assinatura de documentos eletrônicos com verificação da integridade de suas informações. Certificados de tipos S1, S2, S3 e S4 serão utilizados em aplicações como cifragem de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo (ITI, 2006).

Os tipos de A1 a A4 e de S1 a S4 definem escalas de requisitos de segurança nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos (ITI, 2006).

A Tabela 1 mostra as características de cada tipo de certificado:

Tabela1. Tipos de Certificados

Tipo de Certificado	Tamanho da Chave (*bits*)	Processo de Geração	Mídia Armazenadora	Validade Máxima (anos)
A1 e S1	1024	*Software*	Cartão inteligente ou *Token*, ambos sem capacidade de geração de chave e protegidos por senha.	1
A2 e S2	1024	*Software*	Cartão inteligente ou *Token*, ambos sem capacidade de geração de chave e protegidos por senha.	2
A3 e S3	1024	*Hardware*	Cartão inteligente ou *Token*, ambos com capacidade de geração de chave e protegidos por senha ou *hardware* criptográfico aprovado pelo CG da ICP Brasil.	3
A4 e S4	2048	*Hardware*	Cartão inteligente ou *Token*, ambos com capacidade de geração de chave e protegidos por senha ou *hardware* criptográfico aprovado pelo CG da ICP Brasil.	3

Fonte ITI (2006)

As Figuras 8 e 9 mostram um exemplo de um certificado digital emitido no âmbito da ICP Brasil, da forma como é exibido pelo sistema operacional *windows.* Sua emissão foi realizada pela Autoridade Certificadora Certisign SRF, conforme pode ser observado pelo caminho de certificação apontado. Nele identificam-se as principais características descritas anteriormente como data de validade, detalhes do certificado, algoritmo de assinatura, versão, número de série, autoridade emissora e caminho da certificação.

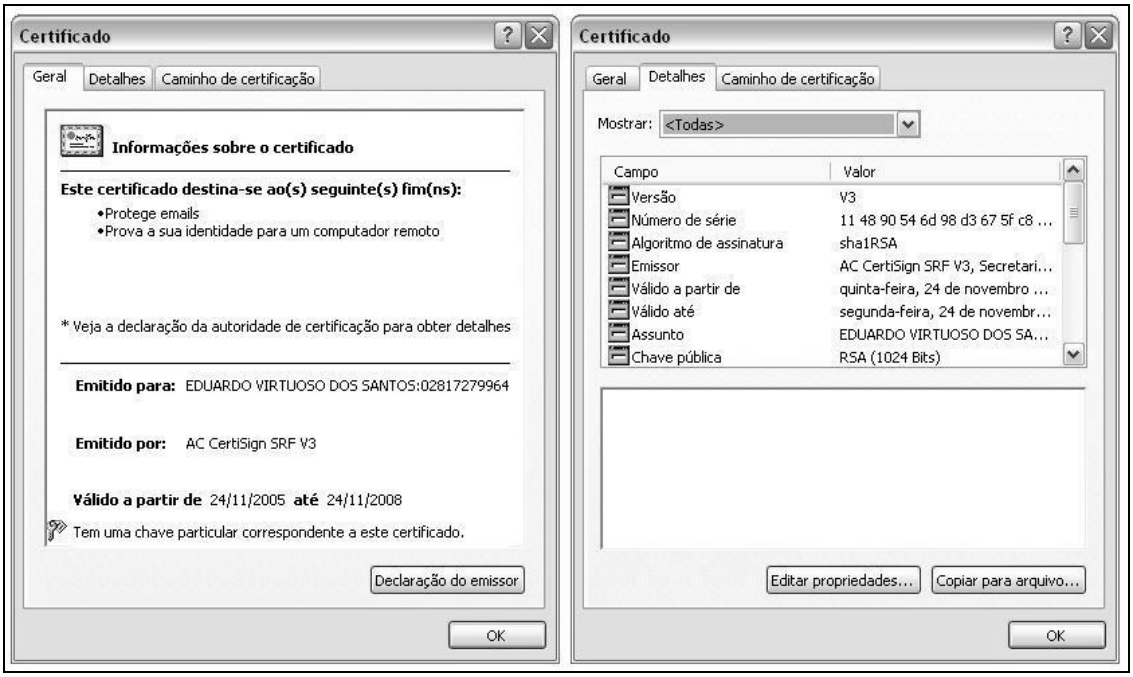

Figura 8. Exemplo de Certificado Digital (Guias Geral e Detalhes)

Figura 9. Exemplo de Certificado Digital (Guia Caminho da certificação)

4 TRABALHOS CORRELATOS

Com a intensificação do uso dos meios eletrônicos para as mais diversas transações, a tecnologia de certificação digital pode ser agregada a várias aplicações, suprindo a carência existente no âmbito da autenticação e do não repúdio de informações.

A seguir serão listados alguns projetos em desenvolvimento nesta área, em nível regional e nacional.

4.1 CARTÓRIO VIRTUAL

A Universidade Federal de Santa Catarina, parceira do Laboratório de Segurança em Computação (LabSEC), do Centro Tecnológico em cooperação com o Laboratório de Informática Jurídica (Linjur) do Centro de Ciências Jurídicas estão desenvolvendo uma tecnologia para fazer os serviços dos cartórios convencionais via Internet. Este cartório abrange vários setores de cartórios convencionais e com o uso da certificação digital pretende disponibilizar estes serviços em meio eletrônico (CUSTÓDIO, 2001).

Os principais serviços a serem disponibilizados são:

a) **títulos e protestos:** abrange o controle de títulos e protestos via *web*. Agiliza e facilita a atividade dos envolvidos com segurança, privacidade e garantia de não repúdio pelas partes;

b) **contratos:** permite a geração de contratos via *web*. Possibilita que as partes envolvidas acessem o contrato, escolham o modelo adequado e, através de sua certificação digital assine-o;

c) **depósito de documentos:** Permite que um usuário deposite no cartório virtual um documento que foi digitalizado. Este documento estará disponível em qualquer filial do cartório, para um outro usuário que necessitar acessá-lo.

4.2 ICP PARA AMBIENTES CORPORATIVOS

Trabalho desenvolvido no curso de engenharia da computação da faculdade de ciências exatas e tecnologia (FAET), no centro universitário de Brasília (UNICEUB). Trata-se de uma abordagem de infra-estrutura de chaves públicas para um ambiente corporativo, visando desenvolver um aplicativo para uso interno em organizações que desejem trocar informações internas com a garantia de autenticidade, confidencialidade e não repúdio.

Nesta abordagem, a própria organização atuará como uma AC, gerando certificados para seus funcionários e, se desejar, para seus clientes e parceiros comerciais, reduzindo o custo de se implementar uma estrutura de chaves públicas já preparada por uma AC comercial. Como as empresas têm tido problemas relacionados a fraudes eletrônicas, este trabalho proporciona uma política de segurança adequada para o uso interno e gera uma economia em gastos que seriam feitos com uma AC externa à organização.

5 CERTIFICAÇÃO DIGITAL NA UNESC

Diante do exposto neste trabalho, percebe-se que a certificação digital através das infra-estruturas de chaves públicas se tornou bastante aceita pela comunidade científica como forma de autenticar usuários em sistemas de informação, bem como garantir a autenticidade de informações encontradas em ambientes virtuais.

Com o desenvolvimento do aplicativo de Diário *On-Line* oferecido aos professores da Unesc, sentiu-se a necessidade de autenticar os participantes do processo que terão acesso as informações deste banco de dados. Dentre as informações constantes neste sistema, estão as notas atribuídas e a freqüência dos alunos matriculados em cada disciplina. Tanto do ponto de vista administrativo, como organizacional, a relevância e o sigilo que merecem estas informações levam a buscar formas de autenticar de maneira confiável os participantes do processo. Desta forma, entendeu-se que a certificação digital pode contribuir para esta finalidade, fornecendo a possibilidade de se certificar todos os envolvidos nas atividades de inserção de dados e atualização do Diário *On-Line*. A partir daí foi necessário iniciar uma pesquisa detalhada sobre as possibilidades de aplicação e a viabilidade das soluções para a Universidade.

Como as soluções oferecidas comercialmente por empresas do ramo de segurança são inviáveis do ponto de vista financeiro, devido ao alto custo dos produtos disponíveis, conforme mostra as Tabelas 2 e 3, iniciou-se contato com os participantes do Grupo de Trabalho da Infra-Estrutura de Chaves Públicas Educacional (ICP EDU), solicitando a participação daquela equipe no sentido de fornecer a estrutura necessária para se implementar a certificação digital na Unesc. Necessidade esta que foi prontamente atendida pelo interlocutor, Professor Dr. Ricardo Felipe Custódio, da

Universidade Federal de Santa Catarina (UFSC). De acordo com o professor, o projeto da ICP EDU pode ser usado para a criação de uma Autoridade de Registro (AR) local, tendo como base a Unesc e com poderes para emitir certificados aos professores e demais funcionários envolvidos com o aplicativo Diário *On-Line*. Solução que atende um dos requisitos necessários para garantir a segurança e sigilo dos dados, resolvendo a questão relativa à autenticação dos usuários.

Por outro lado, como o conteúdo do Diário *On-Line* pode ser acessado remotamente, é necessário que se forneça também uma característica que permita ao usuário ter a certeza de que está acessando a página oficial da Instituição. Esta premissa é alcançada através da certificação do servidor onde está hospedado o serviço e também é fornecida pela ICP EDU. A certificação do servidor através de certificado assinado pela autoridade raiz da ICP EDU garante ao usuário que de fato está acessando a página solicitada em seu navegador. Desta maneira garante-se a autenticidade, integridade e confidencialidade das informações, possibilitando a implantação do referido aplicativo na Universidade e sua utilização imediata.

Da mesma forma, implantando a Autoridade de Registro da ICP EDU na Unesc abre-se um leque de possibilidades de uso desta estrutura para os mais diversos fins organizacionais e acadêmicos. Podendo servir como base para o desenvolvimento de várias aplicações, dentre as quais pode-se destacar:

a) emissão de certificados para autenticação segura de alunos, professores e funcionários nos serviços oferecidos pela Universidade;
b) criação de aplicativos para a comunicação interna autenticada, substituindo os memorandos, cartas e correspondências institucionais em papel;

c) certificação de equipamentos para possibilitar a divulgação de informações relevantes em ambiente virtual;
d) expansão das pesquisas com base em segurança da informação e certificação digital.

5.1 DIFICULDADES ENCONTRADAS

Após definida a implementação na Universidade, iniciou-se contato com os membros da ICP EDU para a realização da proposta e implantação da Autoridade de Registro Local na Unesc. Neste sentido se poderia estudar *in loco* o funcionamento de uma entidade certificadora, de todos os passos para a sua implantação e configuração, acompanhando ainda as rotinas criadas para a emissão dos certificados. Tendo implantada esta entidade tem-se espaço também para manipulá-la e criar diferentes situações necessárias a sua utilização na Unesc o que traz uma grande quantidade de experiências e inovações referentes à segurança da informação em ambientes virtuais. Ainda neste contexto podem-se desenvolver políticas de segurança adequadas ao uso desta plataforma na Universidade e a sua integração com aplicativos internos em funcionamento atualmente. Nos freqüentes contatos com o grupo de trabalho da ICP EDU, através de seu representante na Universidade Federal de Santa Catarina, foi informado que apesar de contar com um pequeno atraso na finalização do projeto, ter-se-iam os sistemas operando em tempo hábil para a conclusão deste trabalho.

Ocorre que o ambiente idealizado pelo Grupo de Trabalho da ICP EDU até o momento não foi disponibilizado para a realização da certificação através de sua estrutura. Fato que demandou a busca por novas soluções e impediu a realização das atividades conforme o planejado. Diante desta dificuldade, cogitou-se desenvolver uma

solução própria para implantar uma autoridade certificadora interna isolada de qualquer infra-estrutura, modelando e escrevendo os códigos para este fim. Porém devido à grandiosidade desta solução que não foi elaborada desde o princípio deste trabalho e ainda considerando-se o curto prazo para a entrega dos resultados propostos, levou a não realização desta tarefa, que será proposta como trabalho futuro. Desta forma, tendo o tempo reduzido para a conclusão do presente projeto, iniciou-se pesquisa junto aos fornecedores de tais soluções comercialmente.

5.2 OPÇÕES OFERECIDAS

No âmbito comercial existem várias empresas que fornecem soluções com base na certificação digital. Estas empresas atuam como Autoridades Certificadoras no âmbito da ICP Brasil e fornecem diversos produtos para garantir a segurança de dados e autenticação de usuários. Dentre as quais pode-se citar a Certisign, Serpro e Serasa. Por trabalharem junto à ICP Brasil, estes fornecedores apenas certificam os usuários no âmbito daquela infra-estrutura. Desta forma, apesar de se ter uma certificação com validade jurídica superior à oferecida pela ICP EDU, a solução se torna inviável financeiramente devido ao custo dos certificados, conforme mostra a Tabela 2. Fica também prejudicada no que tange a necessidade de se buscar pelos serviços de autoridades de registro para a certificação dos usuários. Em qualquer das empresas que poderiam ser escolhidas para realizar a função de certificadora, seria necessário solicitar o deslocamento de um agente de registro para a emissão e entrega dos certificados aos usuários. Atualmente não existe nenhum agente de registro atuando na cidade onde se localiza a sede da Unesc, de forma que não atende as necessidades de certificação constante de novos usuários e a revogação em tempo hábil de certificados

vigentes. Do ponto de vista financeiro, a dificuldade encontra-se na quantidade de certificados que são necessários e ainda no prazo de validade que não pode ser flexibilizado, ocorrendo perdas com certificações usadas em apenas um semestre e pagas por todo o seu período de validade. A quantidade de professores e envolvidos com o processo e necessitados da certificação torna-se o grande empecilho na implantação de qualquer solução oferecida comercialmente.

Na Tabela 2 pode-se observar o comparativo entre os preços de certificados digitais oferecidos a pessoa física, praticados no mercado em novembro de 2006, de acordo com o tipo e prazo de validade.

Tabela 2. Comparativo de Preços de Certificados Pessoais

	Certificado e-CPF A3 em *smart card* (válido por três anos)	Certificado e-CPF A3 em *smart card* com leitora (válido por três anos)	Certificado e-CPF A3 em *token* criptográfico (válido por três anos)	Certificado e-CPF A1 armazenado no próprio computador (válido por um ano)	Certificado e-CPF A3 (apenas o certificado, válido por três anos)
Certisign	R$ 200,00	R$ 350,00	R$ 350,00	R$ 100,00	R$ 150,00
Serasa	R$ 404,00	R$ 460,00	-	R$ 100,00	R$ 380,00
Serpro	-	-	-	R$ 95,00	R$ 125,00

Fonte: CERTISIGN (2006); SERASA(2006); SERPRO (2006)

Após a análise das possibilidades e seus custos, houve um redirecionamento do projeto proposto, iniciando-se a pesquisa com finalidade de se certificar o servidor que abrigará o aplicativo Diário *On-Line*. Esta característica permite que os usuários tenham a certeza de estar acessando a página oficial da instituição e possibilitará que seja atribuído a esta página o *HyperText Transfer Protocol Secure* (HTTPS). Este protocolo permite que a comunicação entre o servidor e o usuário seja realizada através de um sistema seguro de envio e recebimento de mensagens. No tocante a certificação do servidor, encontrou-se algumas opções para a

certificação junto a ICP Brasil, conforme detalhado na Tabela 3. São listados os preços praticados em novembro de 2006 de acordo com tipo e o prazo de validade.

Tabela 3. Comparativo de Preços de Certificados para Equipamentos

	Tipo	Validade	Preço
Site Seguro Pro - Certisign	A3	1 ano	R$ 2.953,50
Site Seguro - Certisign	A3	1 ano	R$ 1.890,00
Web Certisign ICP Brasil	A1	1 ano	R$ 1.890,00
Identificador SERASA	A3	1 ano	R$ 2.750,98
e-Equipamento SERPRO	A1	1 ano	R$ 735,00

Fonte: CERTISIGN (2006); SERASA(2006); SERPRO (2006)

Nota-se que apesar de ser reconhecida juridicamente e comercialmente junto ao ambiente da ICP Brasil, a viabilidade de implantação na Unesc ainda é discutível do ponto de vista financeiro, visto que logo se terá a implantação da certificação através da ICP EDU sem custos para a Universidade e a partir daí a possibilidade de se certificar qualquer equipamento que se julgue necessário.

5.3 SOLUÇÃO ENCONTRADA

Após a avaliação das opções e análise dos tipos de certificação disponíveis para o servidor da Universidade, a alternativa mais viável e com melhor custo benefício envolvido, foi encontrada junto à empresa Certisign Certificadora Digital S.A. que está presente no mercado nacional desde 1996 e é a única habilitada a operar em múltiplas hierarquias, podendo emitir certificados no âmbito da ICP Brasil ou ainda através da *VeriSign Trust Network* da empresa *VeriSign Inc.* líder mundial na prestação de serviços de confiança em redes de comunicação. Trata-se do Certificado *Site* Seguro, que permite a autenticação do servidor e utiliza-se da criptografia nos padrões do protocolo SSL/TLS, que é um protocolo de Internet para criptografia e autenticação baseada em sessão, fornecendo um canal seguro entre o cliente e o servidor. Este

produto permite ainda o uso do selo de *site* seguro Certisign e fecha conexão de 128 *bits* com a quase totalidade dos navegadores disponíveis (CERTISIGN, 2006). Este produto tem o preço inicial de R$ 1.890,00 (mil oitocentos e noventa reais) por servidor e validade de 1 (um) ano, de acordo com pesquisa efetuada no *site* da empresa fornecedora em novembro de 2006.

Seguindo os procedimentos para a aquisição deste certificado foi encontrada a possibilidade oferecida pela empresa de se realizar um teste gratuito do certificado com a finalidade de se adequar os sistemas para receber o certificado oficial e demonstrar o funcionamento do mesmo ou ainda para testar os recursos SSL do servidor *web*. Tal operação pode ser realizada através de uma seqüência de passos que simula o pedido e a instalação de um certificado digital para servidores, com a diferença de que o equipamento será certificado por uma autoridade certificadora sem validade comercial. Esta autoridade deverá ser instalada na raiz de segurança do navegador para o seu correto funcionamento. Os certificados emitidos desta forma têm o prazo de validade reduzido por questões de segurança e funcionam por quatorze dias. Porém pode-se solicitar quantos certificados de teste forem necessários para que se proceda todos os testes e demonstrações necessárias.

Tendo em vista o interesse científico e laboratorial da certificação do servidor e ainda considerando-se que a certificação através das raízes do projeto ICP EDU está prestes a ser disponibilizada, optou-se por este certificado para a conclusão deste projeto. De forma que se possui todas as características de um certificado oficial, portanto sem prejuízo às diretrizes traçadas inicialmente para o estudo e apresentação desta solução. Assim se tem a possibilidade de realizar todas as fases da certificação através de teste e consequentemente a realização do projeto com custo zero para a Universidade.

A seguir, são descritos os procedimentos realizados para a conclusão desta etapa.

5.4 CERTIFICAÇÃO DO SERVIDOR

O servidor utilizado para a realização deste trabalho e que abriga temporariamente no período de testes o aplicativo Diário *On-Line* trabalha com o sistema operacional *Linux Red Hat Entrepise* versão 3, com servidor de página *Apache* 2.0.46.

Após a instalação e configuração do *software* de servidor *web* e a leitura da Declaração das Práticas de Certificação (DPC) da Autoridade Certificadora de Testes que se encontra no anexo A, iniciou-se o processo de solicitação do certificado digital. A maior parte das necessidades será realizada através de linhas de comando. Para se iniciar o processo de certificação deste servidor, foi necessário criar uma chave privada e armazena-la no próprio servidor. A linha de comando utilizada para este fim esta listada abaixo:

/usr/bin/openssl genrsa -des3 -out /etc/httpd/conf/ssl.key/server.key 1024

Ao executar este comando, se fez necessária a criação de uma senha de segurança. Esta senha deve ser digitada sempre que se reiniciar o servidor seguro. A chave com 1024 *bits* foi criada e armazenada em um arquivo chamado de *server.key* no diretório *etc/httpd/conf/ssl.key*. Deve-se fazer uma cópia de segurança deste arquivo e guardá-lo em um lugar seguro, pois após usá-lo para a solicitação do certificado do

servidor ele será necessário para o seu correto funcionamento. Além disso, o arquivo *server.key* deve pertencer à raiz e não deve ser acessível por qualquer usuário.

Após a criação da chave privada, utiliza-se dela como entrada no comando de geração do *Certificate Signing Request* (CSR), ou seja, o pedido de assinatura de certificado. O CSR é um arquivo criptografado que contém a chave pública, nome, localidade e endereço *web* da organização solicitante (CERTISIGN, 2006). O comando utilizado para este fim está descrito abaixo:

/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key -out /etc/httpd/conf/ssl.csr/

Neste momento, foi necessário digitar a senha criada na etapa anterior e mais algumas informações que compõe o pedido de assinatura de certificado. As informações solicitadas foram as seguintes:

a) abreviação do nome do país do solicitante, com duas letras;
b) nome do estado da sede do solicitante, por extenso;
c) nome da localidade do solicitante, por extenso;
d) nome da organização solicitante, por extenso;
e) nome comum do solicitante, *hostname* do servidor;
f) endereço de *e-mail* do solicitante;

Outras informações adicionais também foram solicitadas e por serem opcionais foram deixadas em branco ou com a definição padrão conforme se pode observar na cópia da tela da execução do comando, mostrada na Figura 10.

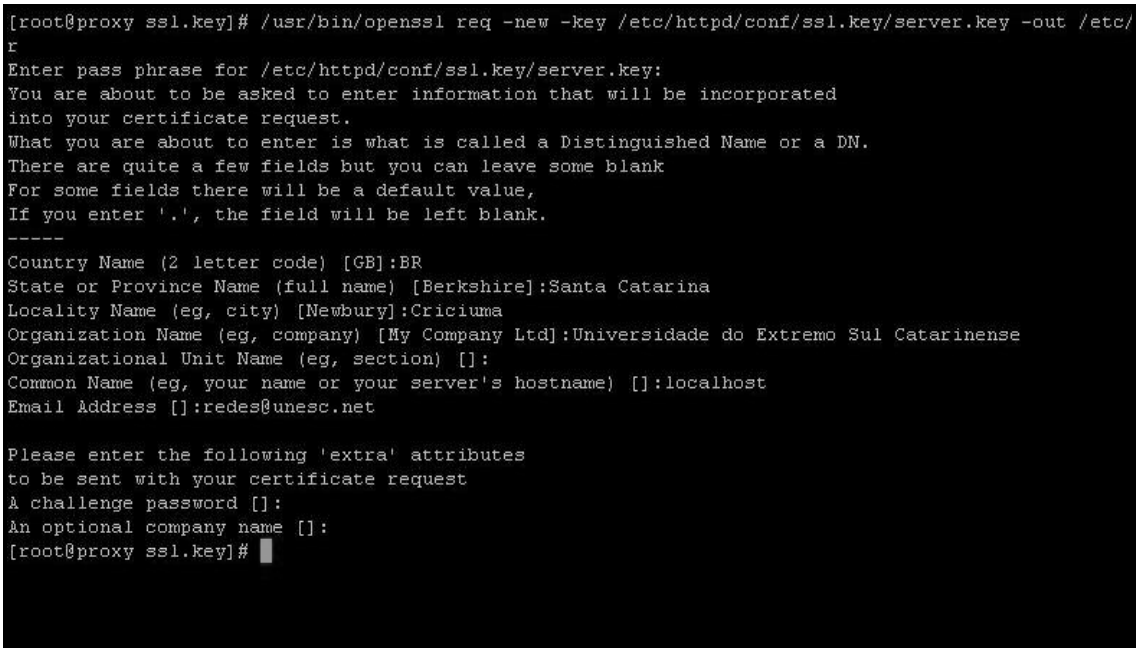

Figura 10. Execução de comando para geração do CSR

Entre as instruções emitidas após executar o comando, o sistema informa que algumas perguntas possuem uma resposta padrão pré-determinada. Esta resposta estará escrita entre colchetes. Se for digitado *enter* nestas opções será assumida a resposta padrão. Para deixá-la em branco deve-se digitar '.' (ponto). Os nomes do estado, localidade e organização devem ser escritos por extenso evitando-se caracteres especiais. No nome do *host* do servidor deve ser digitado o nome real do servidor seguro. Não é necessário resposta em nenhum dos atributos extras, para continuar sem digitar estes dados, basta pressionar a tecla *enter*.

Passo contínuo a digitação das informações solicitadas foi gerado um arquivo chamado *ssl.csr* no diretório */etc/httpd/conf* . Este arquivo contém o pedido de certificado, pronto para ser enviado ao fornecedor. Com este propósito, visualizou-se o conteúdo do arquivo e procedeu-se a cópia dos dados para envio a empresa certificadora. Nesta etapa, realizou-se acesso no endereço listado a seguir para enviar o pedido de assinatura de certificado:

http://www.certisign.com.br/produtos/certificados/siteseguro.jsp#

A Figura 11 mostra um exemplo de como será apresentado os dados no arquivo com a solicitação da assinatura do certificado:

```
 -----BEGIN NEW CERTIFICATE REQUEST----
MIIBCTCBtAIBADBPMQswCQYDVQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTEYMBYG
A1UEChMPRXllcyBvbiBUaGUgV2ViMRQwEgYDVQQDFAt3d3cuZXR3Lm5ldDBcMA0G
CSqGSIb3DQEBAQUAA0sAMEgCQQCeojtjnHqgOGTxp+XZ56RaSe1iZWpumXjU6Sx7
v1FdXzsY1oLOQa090Jtnu1WsQRHhOyDS+45oncjKm1zCG/IZAgMBAAGgADANBgkq
hkiG9w0BAQQFAANBAFBj9g+NiUh8YWPrFGntgf4miUd/wqUshptjJy4PjdsD3ugy
5svvuh3G//PpGh2aYXIjHpJXTUBQyzxSEIINYtc=
 -----END NEW CERTIFICATE REQUEST-----
```

Figura 11. Exemplo de arquivo CSR

Ao se inserir estes dados no formulário da empresa certificadora, deve-se copiar o texto inteiro do certificado, incluindo as linhas -----BEGIN CERTIFICATE REQUEST----- e -----END CERTIFICATE REQUEST-----, porém sem incluir espaço em branco antes dos hífens do início e do final. Nesta etapa foi necessário confirmar os dados apresentados na página da empresa, os quais foram absorvidos através do arquivo de solicitação enviado. Neste momento também foram solicitados o nome do contato técnico e o número de inscrição no CNPJ da organização. Após este procedimento a empresa certificadora enviou um e-mail para o endereço informado no arquivo de solicitação com o certificado assinado. A cópia deste *e-mail* pode ser visualizada no anexo B. Junto com o certificado do servidor, também foi enviado o certificado raiz de teste da empresa certificadora. Fez-se necessária a sua instalação para possibilitar o reconhecimento do certificado do servidor através da cadeia de certificação, visto que a mesma não está fornecida junto com os navegadores comerciais por ser uma autoridade de teste. Sua instalação foi necessária em todos os computadores onde foram efetuados testes com o certificado digital do servidor ou acessada a página segura. Nos testes efetuados com alguns sistemas operacionais, ao se instalar este certificado raiz, são emitidos avisos com a informação de que não podem reconhecer automaticamente esta autoridade certificadora. É informado ainda que ao

prosseguir será instalada uma autoridade raiz e por conseqüência o reconhecimento de todos os certificados assinados por ela como válidos.

Na Figura 12 pode-se visualizar este certificado raiz na forma como é exibido pelo sistema operacional *windows*.

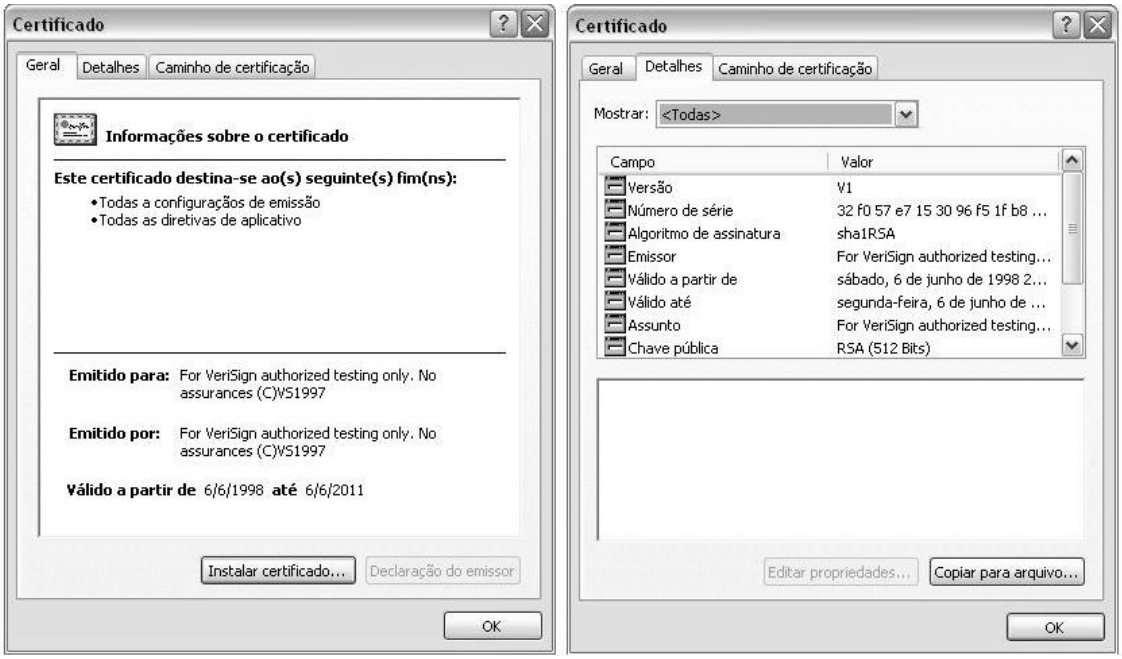

Figura 12. Certificado raiz para testes

Para instalar o certificado digital no servidor, bastou adicionar o conteúdo recebido na mensagem de *e-mail* para o arquivo *server.crt* no diretório */etc/httpd/conf/ssl.crt/*. Neste caso também é necessário que se copie o conteúdo existente desde a linha -----BEGIN CERTIFICATE----- até a linha -----END CERTIFICATE----- para salvá-lo em um arquivo com a extensão CRT.

Após a certificação do servidor e a instalação da autoridade raiz nos computadores usados para o teste iniciou-se a fase conclusiva deste projeto que culminou com o reconhecimento da página que fornece o acesso ao aplicativo Diário *On-Line* como segura, utilizando-se protocolo https como é apresentado na Figura 13.

No navegador *Internet Explorer* utilizado nos computadores do teste esta condição é representada pela figura de um cadeado fechado no rodapé da página.

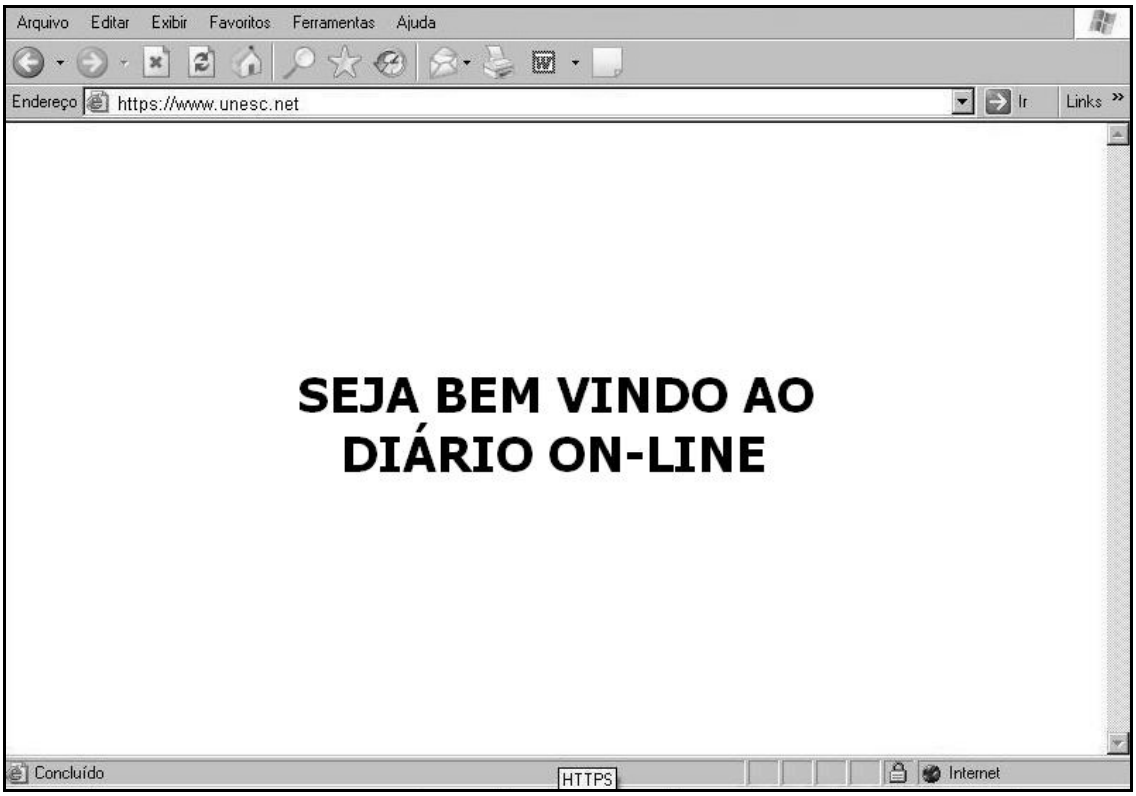

Figura 13. Página de acesso *https*

Para se ter acesso às informações do certificado da página basta clicar no cadeado que será apresentada uma janela com as guias Geral, Detalhes e Caminho de certificação, já demonstradas. Nesta última guia pode-se identificar a autoridade que concedeu o certificado para o servidor, neste caso a *VeriSign*, autorizada apenas para teste conforme mostra a Figura 14.

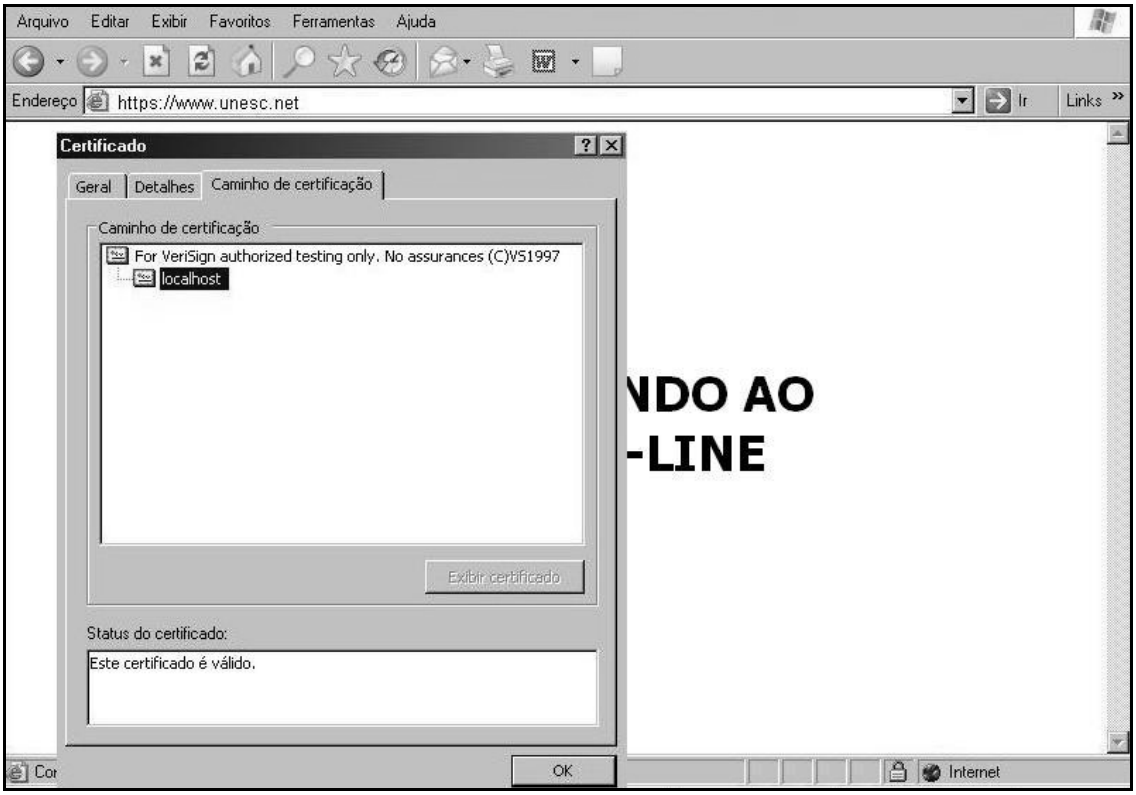

Figura 14. Exibição do certificado

Com esta exibição, o usuário pode certificar-se que está acessando realmente a página oficial e não uma cópia adulterada ou com intenções espúrias. Desta forma concede-se a autenticidade e confidencialidade para o aplicativo Diário *On-Line*.

CONCLUSÃO

Na medida em que são apresentadas novas tecnologias para o armazenamento e distribuição das informações, as aplicações voltadas para garantir a sua segurança mostram-se essenciais e necessárias à sua aceitação pelas comunidades científicas e comerciais.

Com o estudo da criptografia aplicada à certificação digital através dos algoritmos assimétricos, ensaiaram-se as possibilidades de sua aplicação em ambientes corporativos, para a garantia de requisitos como a confidencialidade, a integridade e a autenticidade das informações.

Neste ínterim percebeu-se a importância destas características na apresentação de soluções em tecnologia da informação baseadas nas infra-estruturas de chaves públicas, onde se agregou a validade jurídica atribuída pela ICP Brasil.

Da mesma forma, a capacidade de geração de novos experimentos permitidos pelo desenvolvimento da ICP EDU e sua vinculação com o meio acadêmico, incentiva o estudo desta arquitetura, bem como a sua aplicação nas mais diversas áreas da tecnologia.

Apesar das dificuldades encontradas no intuito de se instalar uma Autoridade Certificadora Local na Universidade, o objetivo deste trabalho foi alcançado com o estudo das possibilidades e a certificação do servidor de dados que abrigará o aplicativo Diário *On-Line* desenvolvido pela Unesc.

Por meio do estudo de caso apresentado conclui-se que a certificação digital permanece como uma forma bastante aceita para promover a segurança em ambientes virtuais, onde se espera que seja mantido o sigilo e a integridade das informações.

Estima-se que este estudo contribua para despertar o interesse em novas pesquisas e na busca por soluções cada vez mais atraentes aos consumidores desta área da informática. No tocante aos desenvolvimentos futuros podem-se sugerir pesquisas com o uso de certificados digitais para a autenticação de usuário em sistemas e a implantação da Autoridade de Certificadora Local na Unesc, visto que logo será disponibilizado aos acadêmicos toda a estrutura operacional da ICP EDU. Esta possibilidade fornece aos pesquisadores uma infinidade de aplicações com base na referida infra-estrutura e suas ramificações. Uma grande contribuição para o crescimento e desenvolvimento regional apoiados pela Universidade.

Finalmente, entende-se que este trabalho além de despertar o interesse pela pesquisa e por novas descobertas, contribuiu na formação e no desempenho profissional do acadêmico, notadamente através de sua atuação como agente de registro no âmbito da Infra-estrutura de Chaves Públicas Brasileira.

REFERÊNCIAS

BRASIL. Medida Provisória nr. 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 Ago. 2001.

BUCHMANN, Johannes A. **Introdução à criptografia.** São Paulo: Berkeley, 2002.

CARVALHO, Daniel Balparda de**. Criptografia: métodos e algoritmos.** 2.ed Rio de Janeiro: Book Express, 2001.

CERTISIGN. **Certisign Certificadora Digital**. São Paulo - Brasil, 2006. Disponível em: <http://www.certisign.com.br>. Acesso em: 30 Out 2006.

CUSTÓDIO, Ricardo Felipe; GRAAF, Jeroen Van de; DAHAB, Ricardo. **Uma Infra-Estrutura de Chaves Públicas para o Âmbito Acadêmico**. Florianópolis: UFSC, 2003.

FORD, W.; BAUM, M. ***Secure Electronic Commerce.*** New Jersey: Prentice-Hall, 2000.

GARFINKEL, S; SPAFFORD, G. **Comércio & Segurança na *WEB*.** 1. ed. São Paulo: Market Books, 1999.

HOUAISS, Antônio. **Dicionario houaiss da língua portuguesa**: Antônio Houaiss. Rio de Janeiro: 1994. Objetiva, 2001.

ITI. **Instituto Nacional de Tecnologia da Informação**. Brasília - Brasil, 2006. Disponível em: <http://www.iti.br>. Acesso em: 01 Out 2006.

SERASA. **Portal Serasa.** São Paulo - Brasil, 2006. Disponível em: <http://www.serasa.com.br>. Acesso em: 30 Out 2006.

SERPRO. **Serviço Federal de Processamento de Dados.** Brasília - Brasil, 2006. Disponível em: <http://www.serpro.gov.br>. Acesso em: 30 Out 2006.

SILVA, Lino Sarlo da. **Public Key Infrastructure.** São Paulo: Novatec, 2004.

STALLINGS, William. ***Cryptography and network security: principles and practice.*** 2.ed. New Jersey: Prentice Hall, 1998.

STINSON, Douglas R. ***Cryptography: theory and practice.*** Boca Raton: CRC-SP, 1995

TRAIN, Sheila. **Identidade Digital.** São Paulo: Certising, 2005.

BIBLIOGRAFIA RECOMENDADA

BRASIL. Lei nr. 6.015, de 31 DE DEZEMBRO DE 1973, Lex: Dispõe sobre os registros públicos, e dá outras providências. Brasília, 1973.

BRASIL. Lei nr. 8.935, DE 18 DE NOVEMBRO DE 1994, Lex: Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro. Brasilia, 1994.

BURNETT, Steve; PAINE, Stephen. **Criptografia e segurança: o guia oficial RSA.** Rio de Janeiro: Elsevier, 2002.

CRONKHITE, Cathy; MCCULLOUGH, Jack. **Hackers, acesso negado : o guia completo para a proteção dos seus negócios on-line.** Rio de Janeiro: Campus, 2001.

ICP BRASIL. **Infra-estrutura de chaves públicas Brasileira**. Brasília - Brasil, 2006. Disponível em: <http://www.icpbrasil.gov.br>. Acesso em: 01 Out 2006.

ICP EDU. **Infra-estrutura de chaves públicas Educacional**. Florianópolis - Brasil, 2006. Disponível em: <http://www.icpedu.labsec.ufsc.br>. Acesso em: 01 Out 2006.

PEREIRA, Fernando Carlos. **Criptografia Temporal: Aplicação Prática em Processos de Compra.** Florianópolis: UFSC, 2003.

PROSISE, Chris. **Hackers: resposta e contra-ataque.** Rio de Janeiro: Campus, 2001.

STALLINGS, William. **Data and computer communications.** 5.ed New Jersey: Prentice Hall, 1997.

STALLINGS, William. **Network security essentials: applications and standards.** New Jersey: Prentice Hall, 2000.

ANEXO A – DECLARAÇÃO DAS PRÁTICAS DE CERTIFICAÇÃO DA AC DE TESTE

Certisign Certificadora Digital S/A AUTORIDADE DE CERTIFICAÇÃO DE TESTE

DECLARAÇÃO DAS PRÁTICAS DE CERTIFICAÇÃO

VERSÃO 1.0

LEIA ATENTAMENTE ESTA DECLARAÇÃO DAS PRÁTICAS DA AUTORIDADE CERTIFICADORA (AC) DE TESTE Certisign Certificadora Digital S/A. AO CLICAR ABAIXO EM ACEITAR E/OU SOLICITAR, OU AO CONFIAR NUM CERTIFICADO DE TESTE OU NO CERTIFICADO RAIZ DA AC DE TESTE (DE ACORDO COM AS DEFINIÇÕES ABAIXO), O TITULAR CONCORDA EM TORNAR-SE PARTE INTERESSADA DA PRESENTE DPC DE TESTE E OBRIGA-SE COM RELAÇÃO AOS SEUS TERMOS . CASO NÃO CONCORDE COM OS TERMOS DESTA DPC DE TESTE, NÃO SOLICITE, UTILIZE OU CONFIE NUM CERTIFICADO DE TESTE, NO CERTIFICADO RAIZ DA AC DE TESTE, OU EM QUALQUER OUTRO COMPONENTE A ELES ASSOCIADO.

Esta DPC de Teste estabelece os termos e condições pelos quais a Autoridade Certificadora de Teste Certisign Certificadora Digital S/A emite e gerencia Certificados Digitais de Teste para Servidores e as regras de utilização destes Certificados de Teste e do Certificado Raiz de da AC de Teste.

Considera-se Titular do Certificado a pessoa física ou jurídica para a qual e em nome da qual tenha sido emitido um Certificado de Teste, que tenha capacidade ou esteja autorizada a utilizar a chave privativa que corresponde à chave pública listada no Certificado de Teste. O Certificado de Teste permite que o Titular simule a operação de um site oferecendo determinada segurança nas comunicações quando um Certificado Digital de Servidor é adequadamente utilizado. A Certisign Certificadora Digital S.A. disponibiliza o Certificado Raiz da AC de Teste em seu site para fins de testes autorizados e somente de acordo com os termos desta DPC de Teste.

O indivíduo que faz o download e/ou utiliza o Certificado Raiz da AC de Teste, incluindo, sem limitar-se aos funcionários ou outros representantes do Titular, pode simular o processo através do qual o software de navegação autentica as mensagens e estabelece um canal seguro de comunicação para sites que utilizem um Certificado Digital de Servidor.

Esta DPC de Teste fixa obrigações das Partes interessadas e serve como meio de informação aos Titulares e outros Usuários dos Certificados de Teste emitidos por Certisign Certificadora Digital S.A.

Considerando os compromissos fixados nesta DPC de Teste e sua aceitação para todos os fins legais, Certisign Certificadora Digital S.A., Titulares e Usuários concordam com os seguintes termos:

1. USO RESTRITO PARA FINS DE TESTE AUTORIZADO

OS CERTIFICADOS DE TESTE E O CERTIFICADO RAIZ DA AC DE TESTE DEVEM SER UTILIZADOS, EXCLUSIVAMENTE, PARA FINS DE TESTE. OS CERTIFICADOS DE TESTE, O CERTIFICADO RAIZ DA AC DE TESTE E TODOS OS SEUS COMPONENTES NÃO DEVEM SER UTILIZADOS E NEM CONFIADOS PARA QUAISQUER OUTRAS FINALIDADES, INCLUINDO TRANSAÇÕES COMERCIAIS, AUTENTICAÇÃO DA IDENTIDADE DO TITULAR OU DA AC DE TESTE, OU EM GARANTIA DE CONFIDENCIALIDADE DE QUAISQUER INFORMAÇÕES FORNECIDAS PARA EMISSÃO OU UTILIZAÇÃO.

NÃO SOLICITE NEM UTILIZE O CERTIFICADO DE TESTE OU O CERTIFICADO RAIZ DA AC DE TESTE PARA QUAISQUER OUTROS FINS ALÉM DO TESTE AUTORIZADO.

OS TITULARES E OS USUÁRIOS RECONHECEM QUE NEM A IDENTIDADE NEM A AUTORIDADE DOS TITULARES FOI VERIFICADA OU COMPROVADA PELA AC DE TESTE OU PELA Certisign Certificadora Digital S.A.

2. EMISSÃO E USO
Após o recebimento e aprovação da Certisign Certificadora Digital S.A. de uma solicitação de emissão de Certificado de Teste, a Certisign Certificadora Digital S.A. emitirá um Certificado de Teste para o solicitante.

A Certisign Certificadora Digital S.A. fornecerá, também, acesso ao Certificado Raiz da AC de Teste ao Titular e demais Usuários.

Os Certificados de Teste e o Certificado Raiz da AC de Teste deverão ser utilizados exclusivamente para fins de testes autorizados para simulação do processo pelo qual o software de navegação autentica e estabelece um canal seguro para comunicações eletrônicas realizadas através de um site que utilize adequadamente uma identidade certificada por um Certificado Digital de Servidor.

3. SUSPENSÃO E/OU REVOGAÇÃO DE CERTIFICADOS
Os Titulares e Usuários reconhecem que a Certisign Certificadora Digital S.A. não tem a obrigação de suspender ou revogar Certificados de Teste a pedido do Titular. A Certisign Certificadora Digital S.A. está autorizada, a seu critério exclusivo, a revogar todos ou qualquer Certificado de Teste.

4. AUTORIZAÇÃO PARA PUBLICAÇÃO DE INFORMAÇÕES
Certisign Certificadora Digital S.A. estará autorizada a publicar ou divulgar qualquer Certificado de Teste ou qualquer parte do conteúdo de um Certificado, no que diz respeito à divulgação das informações contidas ou sobre o Certificado de Teste da Certisign Certificadora Digital S.A. dentro e fora da hierarquia da AC de Teste da Certisign Certificadora Digital S.A.

5. EXCLUSÃO DE GARANTIAS
Certisign Certificadora Digital S.A. EMITE CERTIFICADOS DE TESTE "NO ESTADO". A Certisign Certificadora Digital S.A. NÃO OFERECE QUALQUER GARANTIA EM RELAÇÃO AOS SERVIÇOS FORNECIDOS Certisign

Certificadora Digital S.A. NOS TERMOS DESTA DPC, INCLUINDO EVENTUAIS GARANTIAS DE COMERCIABILIDADE OU ADEQUAÇÃO A UM PROPÓSITO EM PARTICULAR.

Certisign Certificadora Digital S.A. NÃO IDENTIFICA NEM GARANTE A QUALQUER PESSOA QUE QUALQUER TITULAR PARA QUEM TENHA EMITIDO UM CERTIFICADO DE TESTE SEJA DE FATO A PESSOA OU ORGANIZAÇÃO QUE ALEGA SER NAS INFORMAÇÕES DADAS À Certisign Certificadora Digital S.A., OU QUE QUALQUER PESSOA OU EMPRESA SEJA DE FATO A PESSOA OU ORGANIZAÇÃO NOMEADA NUM CERTIFICADO DE TESTE OU NO CERTIFICADO RAIZ DA AC DE TESTE.

Certisign Certificadora Digital S.A. NÃO FORNECE GARANTIAS SOBRE A VERACIDADE, AUTENTICIDADE, INTEGRIDADE OU CONFIABILIDADE DAS INFORMAÇÕES CONTIDAS EM CERTIFICADOS DE TESTE OU NO CERTIFICADO RAIZ DA AC DE TESTE, OU SOBRE OS RESULTADOS DE MÉTODOS CRIPTOGRÁFICOS IMPLEMENTADOS EM CONEXÃO COM TAIS CERTIFICADOS.

NENHUMA INFORMAÇÃO OU RECOMENDAÇÃO ORAL OU ESCRITA FORNECIDA PELA Certisign Certificadora Digital S.A., SEUS FUNCIONÁRIOS OU REPRESENTANTES SIGNIFICARÁ FIXAÇÃO DE QUALQUER GARANTIA OU DE ALGUMA FORMA AUMENTARÁ O ESCOPO DAS OBRIGAÇÕES DA Certisign Certificadora Digital S.A.

6. LIMITAÇÃO DE RESPONSABILIDADE
NENHUMA DAS PARTES SERÁ RESPONSÁVEL POR QUAISQUER DANOS DIRETOS OU INDIRETOS, ESPECIAIS OU INCIDENTAIS, CAUSADOS OU RESULTANTES DA UTILIZAÇÃO DOS CERTIFICADOS DE TESTE.

7. EXPIRAÇÃO DO CERTIFICADO
OS CERTIFICADOS DE TESTE E AS OBRIGAÇÕES DAS PARTES NOS TERMOS DESTA DPC DE TESTE EXPIRARÃO EM DUAS (2) SEMANAS A PARTIR DA EMISSÃO DO CERTIFICADO.

8. EXPIRAÇÃO E/OU REVOGAÇÃO
Certisign Certificadora Digital S.A. RESERVA-SE O DIREITO DE REVOGAR UM CERTIFICADO DE TESTE E RESCINDIR SUAS OBRIGAÇÕES EM RELAÇÃO A UM TITULAR NOS TERMOS DESTA DPC DE TESTE A SEU CRITÉRIO EXCLUSIVO E A QUALQUER MOMENTO, COM OU SEM MOTIVO.
APÓS A EXPIRAÇÃO OU REVOGAÇÃO, POR QUALQUER MOTIVO, DE UM CERTIFICADO DE TESTE, ESTES OU SEUS COMPONENTES NÃO PODERÃO MAIS SER UTILIZADOS OU CONFIADOS PARA QUALQUER FINALIDADE.
A EXPIRAÇÃO OU REVOGAÇÃO DO CERTIFICADO NÃO AFASTA AS DISPOSIÇÕES E OBRIGAÇÕES FIXADAS NAS SEÇÕES 4, 5, 6, 8, E 9 DESTA DPC DE TESTE E NAS RESPECTIVAS SUBSEÇÕES, QUE CONTINUARÃO EM PLENO VIGOR E COM A EFICÁCIA NECESSÁRIA E SUFICIENTE PARA PERMITIR O INTEGRAL CUMPRIMENTO DA PRESENTE.
OS USUÁRIOS DEVERÃO EXCLUIR O CERTIFICADO RAIZ DA AC DE TESTE DE SEUS SOFTWARES DE NAVEGAÇÃO APÓS O TÉRMINO DO TESTE.

9. DISPOSIÇÕES GERAIS

9.1 LEGISLAÇÃO APLICÁVEL

AS LEIS BRASILEIRAS REGULAM A VALIDADE DESTA DPC DE TESTE E DE SEUS TERMOS, SUA INTERPRETAÇÃO E O CUMPRIMENTO DOS DIREITOS E OBRIGAÇÕES DAS PARTES INTERESSADAS.

9.2 SUCESSORES E CESSIONÁRIOS

Este Acordo obriga as Partes interessadas e seus sucessores, testamenteiros, herdeiros, representantes, administradores ou cessionários O Titular e/ou Usuário do Certificado de Teste não pode onerar ou ceder o Certificado ou qualquer direito ou obrigação fixado nesta DPC Qualquer tentativa de cessão ou delegação será nula e ineficaz.

9.3 INDEPENDÊNCIA DAS CLÁUSULAS

Caso qualquer cláusula desta DPC de Teste, ou sua aplicação, for declarada , no todo ou em parte, inválida ou inexigível, nos termos da lei, as demais disposições não serão afetadas e esta DPC deverá ser interpretada de forma a preservar a intenção das partes.
FICA EXPRESSAMENTE ENTENDIDO QUE AS CLÁUSULAS DESTA DPC DE TESTE QUE ESTABELECEM LIMITAÇÕES OU EXCLUSÃO DE RESPONSABILIDADE, GARANTIAS OU REPARAÇÃO DE DANOS, SÃO INDEPENDENTES ENTRE SI E DE QUALQUER OUTRA CLÁUSULA E COMO TAL SERÃO EXECUTADAS.

9.4 CONTRATO INTEGRAL

Esta DPC de Teste constitui o acordo completo entre as Partes interessadas com respeito ao Certificado de Teste e assuntos correlatos tratados nesta DPC, revogando todo e qualquer outro acordo ou entendimentos oral e/ou escrito, anterior e/ou atual, entre as partes.

9.5 NOTIFICAÇÕES

Todas as notificações e avisos relevantes relativamente a esta DPC e ao Certificado de Teste emitido deverão ser feitas por escrito, endereçadas à Certisign Certificadora Digital S.A e enviadas através de correspondência registrada e com recibo de recebimento, ou através de Cartório de Títulos e Documentos, no endereço de sua sede de Certisign à Rua da Passagem 123 - Botafogo - Rio de Janeiro - RJ.

9.6 MARCAS E NOMES COMERCIAIS

O Titular do Certificado de Teste e a Certisign Certificadora Digital S.A. não adquirirão, por motivo desta DPC de Teste ou de sua execução, qualquer tipo de direito sobre qualquer marca, marca de empresa, logomarca ou nome de produto pertencente à outra parte, a sua beneficiária ou a suas prestadoras de serviço, e não farão qualquer uso dos mesmos por qualquer razão, exceto se de outro modo autorizadas por escrito

pela Parte que detenha os direitos de tais marcas, nomes comerciais, logomarcas ou nomes de produto.

ANEXO B – *E-MAIL* RECEBIDO DA AUTORIDADE CERTIFICADORA

Prezado cliente,

Parabéns -- seu Certificado Digital de Servidor de Teste, emitido para www.unesc.net, está incluso no fim desta mensagem.
A CertiSign assinou digitalmente seu Certificado, garantindo que o mesmo não foi danificado ou alterado de forma imperceptível.

Se você não instalou a Raiz da AC (Autoridade Certificadora) de Teste terá que fazê-lo antes de usar seu Certificado Digital Experimental de Servidor.
Você precisará que a Raiz da AC de Teste esteja instalada em cada navegador que irá usar no teste. Para fazer o download da Raiz da CA de teste vá para:
https://digitalid.certisign.com.br/trial/trialserver/trialStep4.htm

Para obter instruções sobre como instalar seu Certificado Digital de Servidor de Teste, por favor visite:
https://digitalid.certisign.com.br/trial/trialserver/trialStep5.htm

Depois que você testar seu Certificado Digital Experimental de Servidor, nós o incentivamos a obter um Certificado Digital de Servidor Seguro totalmente funcional, com validade de um ano, ao visitar:
https://digitalid.certisign.com.br/server/server/enrollIntro.htm

Seu Certificado Digital de Servidor Seguro será assinado digitalmente na VTN - VeriSign Trust Network (Rede de Confiança Global da VeriSign), permitindo imediatamente que milhões de navegadores em uso em toda a Internet realizem conexões seguras com seu site Web.